LA-UR-19-23748
Approved for public release; distribution is unlimited.

Title: Cyber Fire Entry Point Course

Author(s): Pope, Aaron Scott
Wernicke, James
Arias, Pablo
Beck, Shannon Irene
Pickett, Neale T.
Ferrell, Paul Steven

Intended for: Cyber Fire 14, 2019-04-29/2019-05-03 (Atlanta, Georgia, United States)

Issued: 2019-11-12 (rev.1)

Cyber Fire
Entry Point Course

Instructors:
Aaron Scott Pope <apope@lanl.gov>
James Wernicke <wernicke@lanl.gov>
Pablo Arias <arias13@llnl.gov>
Heather Keaty <hkeaty@lanl.gov>

Additional Content Creators:
Shannon Beck <shannon@lanl.gov>
Neale Pickett <neale@lanl.gov>
Paul Ferrell <pferrell@lanl.gov>

“Given enough time, any man may master the physical. With enough knowledge, any man may become wise. It is the true warrior who can master both….and surpass the result.” – Tien T’ai

What is Cyber Fire Foundry?

- Cyber Fire Foundry guides you through creating custom solutions for investigating cybersecurity incidents.
- Rather than teach recipes for yesterday's problems, our veteran staff helps you develop the ability to create innovative solutions to pick apart whatever arrives after you leave our event.

What is Entry Point?

- Introduction to cybersecurity incident investigation
- Broad, but shallow, exposure to the three Cyber Fire categories:
  - Host forensics
  - Network archeology
  - Malware analysis
- Targeted at novices or those wanting *some* exposure to all the categories
- If you don't think you're in the right class, talk to us!

Topic Outline

- Working in Linux
- File Analysis
  - Signatures
  - Metadata
  - Hashing
- Host Forensics
  - Order of Volatility
  - Memory Forensics
  - Forensic Disk Imaging
- Networking Overview
  - Networking Stack
  - Packet Capture
  - Routing and Protocols
- Network Scanning
- Malware Analysis
- File Carving
- Incident Reporting

Hands On Training

Throughout the course, we will include a set of puzzles at the end of each topic. These puzzles will reinforce the core concepts you previously learned with hands on exercises.

https://entrypoint.cyberfire.training

Workstation Introduction

Created by:
Aaron Scott Pope <apope@lanl.gov>

SIFT Workstation

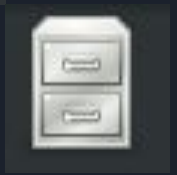
- Built from Ubuntu Linux
- Developed and maintained by SANS
- Includes digital forensics toolkit and helpful guides
- The VM provided has a couple additional tools

Getting Around in the SIFT Workstation

Application search/launcher

Terminal (command prompt)

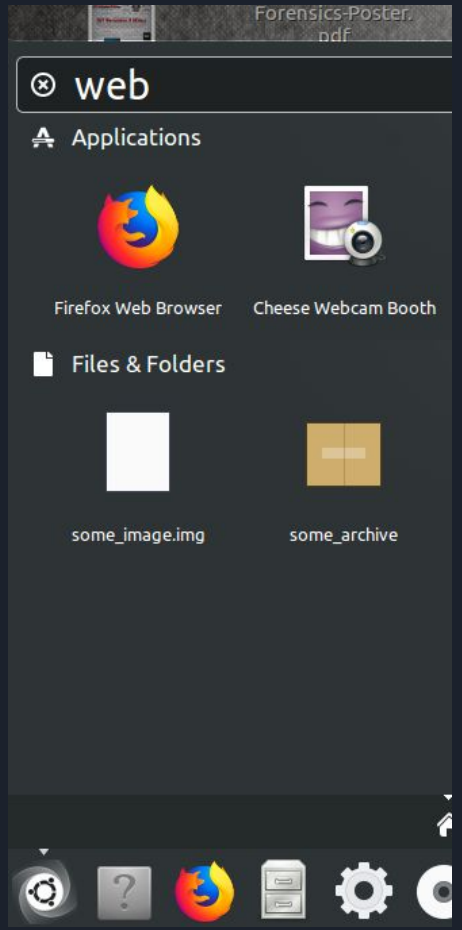
Web browser



File manager

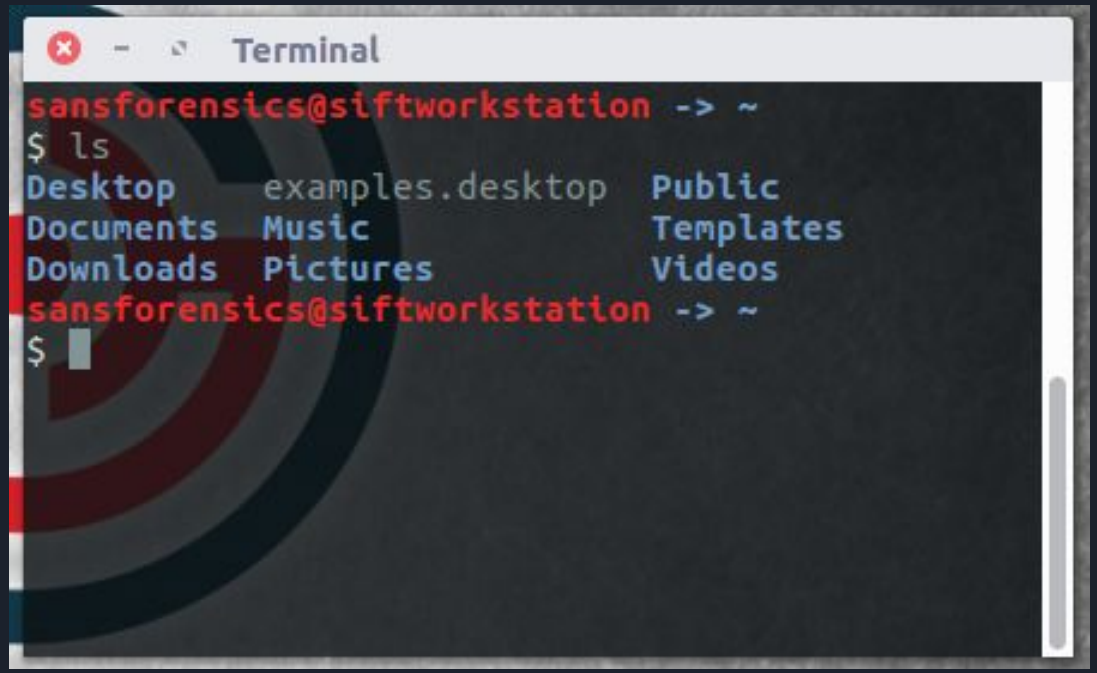
Search Your Computer

Search for programs and files



Terminal Window

Execute command line utilities



Navigating the Command Line

- pwd - Print working directory
- ls - List current directory contents
- cd - Change directory
- mkdir - Make directory
- rmdir - Remove empty directory
- cp - Copy file/directory
- mv - Move file/directory
- rm - Remove file
- cat - Print file contents to the screen
- man - View manual page for a program/command

Exercise Time

Puzzle category:

- IntroToLinux

If you get bored:

- IntroToProgramming

Entry Point

File Analysis

Created by Aaron Pope | apope@lanl.gov

File Types

- Pictures: JPEG, PNG, BMP
- Documents: DOCX, PDF
- Programs: EXE
- Archives: ZIP, TAR

File Extensions

- Windows uses file name suffix or “extension” to determine file type
- Tells Windows how to use the file (what program)
- Can be easily changed to hide the nature of a file (e.g., virus.exe → totally_not_a_virus.txt)

File Signatures

- Non-Windows operating systems typically rely on file “signatures”
- AKA “file magic” or “magic numbers”
- Not as easy to change (doing so usually breaks the file)

File Signatures

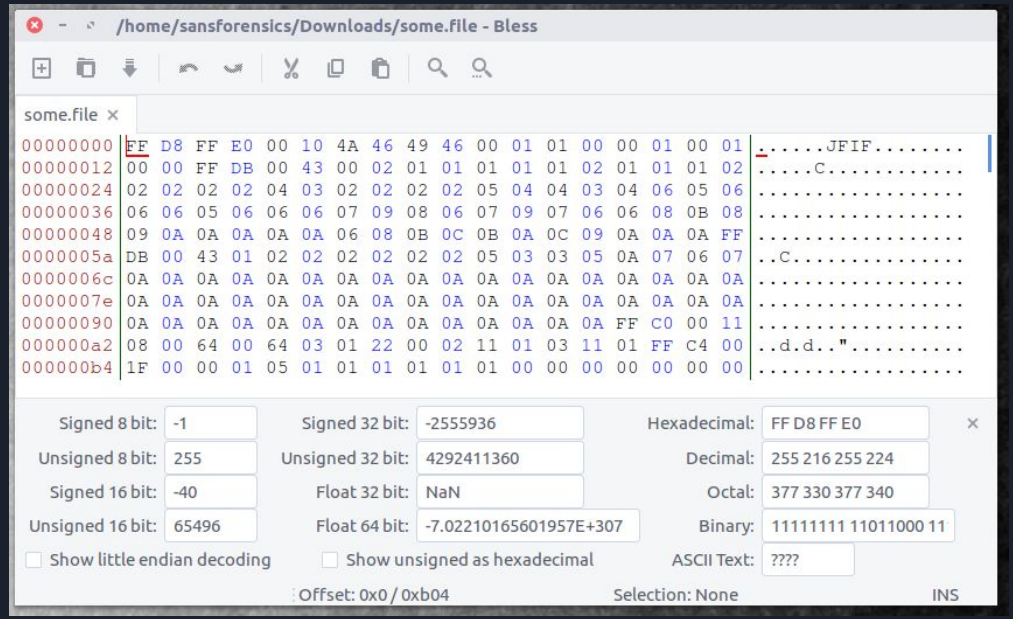
- Information at the beginning (and sometimes end) of a file
- View the file in a hex editor (e.g., Bless)
- Common file signatures can be found online: www.garykessler.net/library/file_sigs.html

Why Do File Signatures Matter?

- Can identify file type when extension has been removed or modified to hide the nature of the file
- Can be used to reconstruct files from raw data when file meta-information is lost
  - Corrupted or deleted data
  - Extracting files from memory image

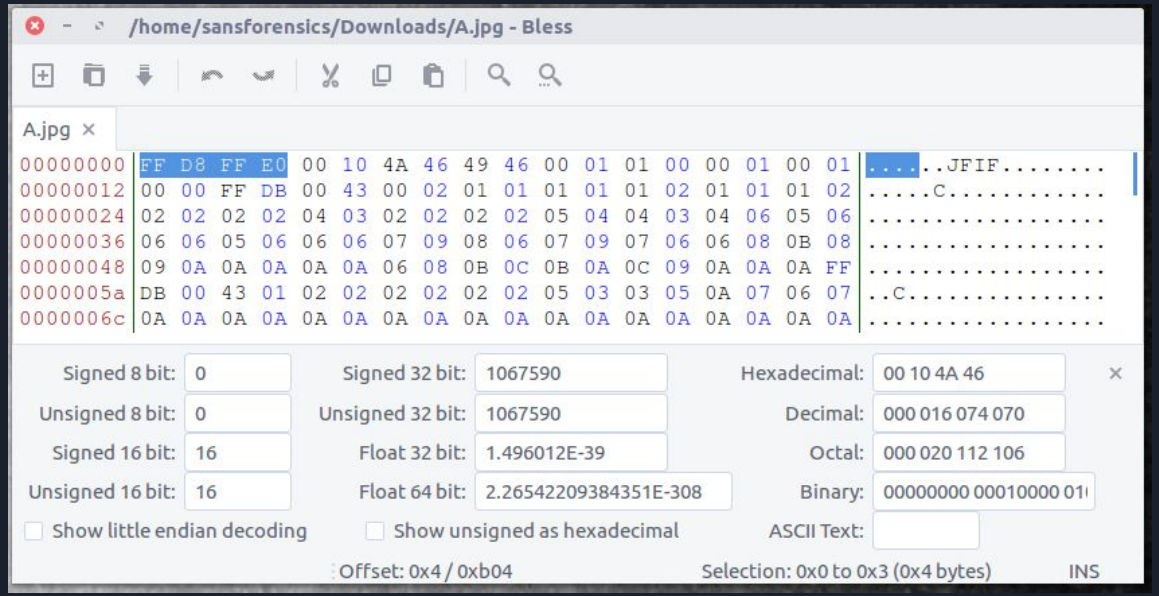
Hex Editor (Bless)

- Displays raw binary contents
- Translates contents into ASCII (text)



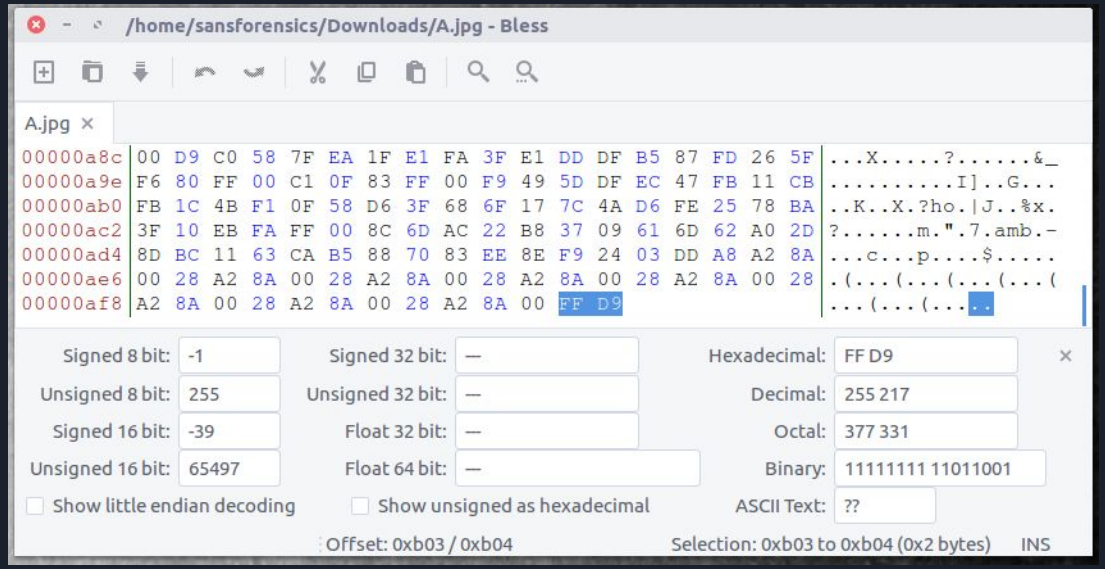
Viewing File Signatures

Example JPEG image file (.jpg) begins with FF D8 FF E0 (file header)



Viewing File Signatures

Some file formats, such as JPEG images, also include file trailers



Common File Signatures

File type	Extension	Signature
JPEG Image	.jpg	FF D8 FF E0
Win/DOS Executable	.exe	4D 5A
Zip Compressed File	.zip	50 4B 03 04
GIF Image	.gif	47 49 46 38
PDF Document	.pdf	25 50 44 46

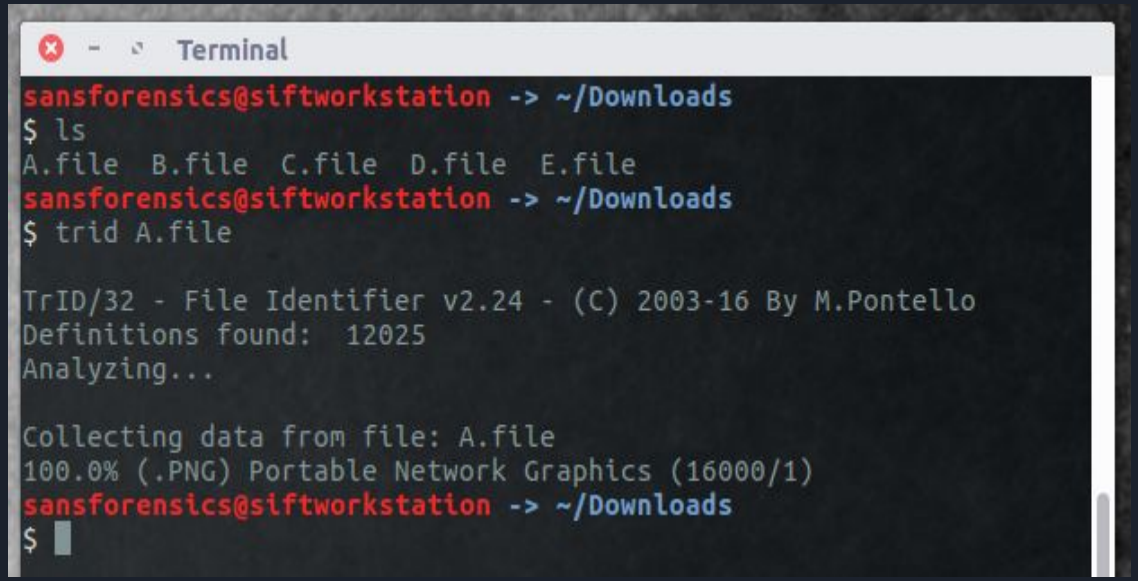
Find other common file signature formats:
www.garykessler.net/library/file_sigs.html

Automated File Signature Analysis

- Linux file command reads file signatures
- Windows versions can be found (gnuwin32.sourceforge.net/packages/file.htm)

Automated File Signature Analysis

- TrID File Identifier
- Uses logic to guess file type from signatures



File Meta-Information

- Some file types have extra (meta) information stored in their file headers
- Examples:
  - GPS coordinates stored in pictures taken by phones/digital cameras
  - PDF Author information

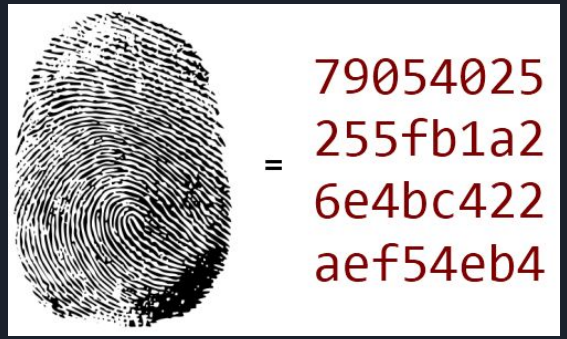
ExifTool

View and modify file meta-information

```
Terminal
sansforensics@siftworkstation -> ~/Downloads
$ ls
A.file  B.file
sansforensics@siftworkstation -> ~/Downloads
$ exiftool A.file
ExifTool Version Number         : 10.10
File Name                       : A.file
Directory                       : .
File Size                       : 8.7 kB
File Modification Date/Time     : 2019:10:21 22:55:09+00:00
File Access Date/Time           : 2019:10:21 22:55:09+00:00
File Inode Change Date/Time     : 2019:10:21 22:55:12+00:00
File Permissions                : rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.3
Linearized                      : No
Title                           : A
Create Date                     : 2017:02:03 15:31:56
Modify Date                     : 2017:02:03 15:31:56
Producer                        : ImageMagick 6.8.9-9 Q16 x86_64 2
016-11-29 http://www.imagemagick.org
Page Count                      : 1
XMP Toolkit                     : Image::ExifTool 10.10
Author                          : Aaron Pope
sansforensics@siftworkstation -> ~/Downloads
$
```

File Hashing

- Generates a "fingerprint" used to identify files
- Based on contents of a file; name not included
- Small change to the contents = big change to the hash
- Commonly used file hash techniques:
  - MD5
  - SHA-1
  - SHA-256
  - SHA-512



File Hashing on Linux

```
sansforensics@siftworkstation -> ~/Documents
$ md5sum hashme.txt
a20ebd903d5d2409048af4fc95612cdf  hashme.txt
sansforensics@siftworkstation -> ~/Documents
$ sha1sum hashme.txt
bd562574087af3144d618fa1764f47703f99e7e9  hashme.txt
sansforensics@siftworkstation -> ~/Documents
$ sha256sum hashme.txt
b6ef88944be8d3d9b28985da2c4388cccd102a97b0cc649c595b33d7afd12503  hashme.txt
sansforensics@siftworkstation -> ~/Documents
$ sha512sum hashme.txt
0d26b4cf87116e14a8320bd02c6cd8019f2698ec8a005657d36a4f66dfdac000bfaa4c87edcf6b0bc4501382cc
66fc0c9086cba73148de78e5cae2e932f3cc5c  hashme.txt
sansforensics@siftworkstation -> ~/Documents
$
```

Exercise Time

Puzzle category:

- FileAnalysis

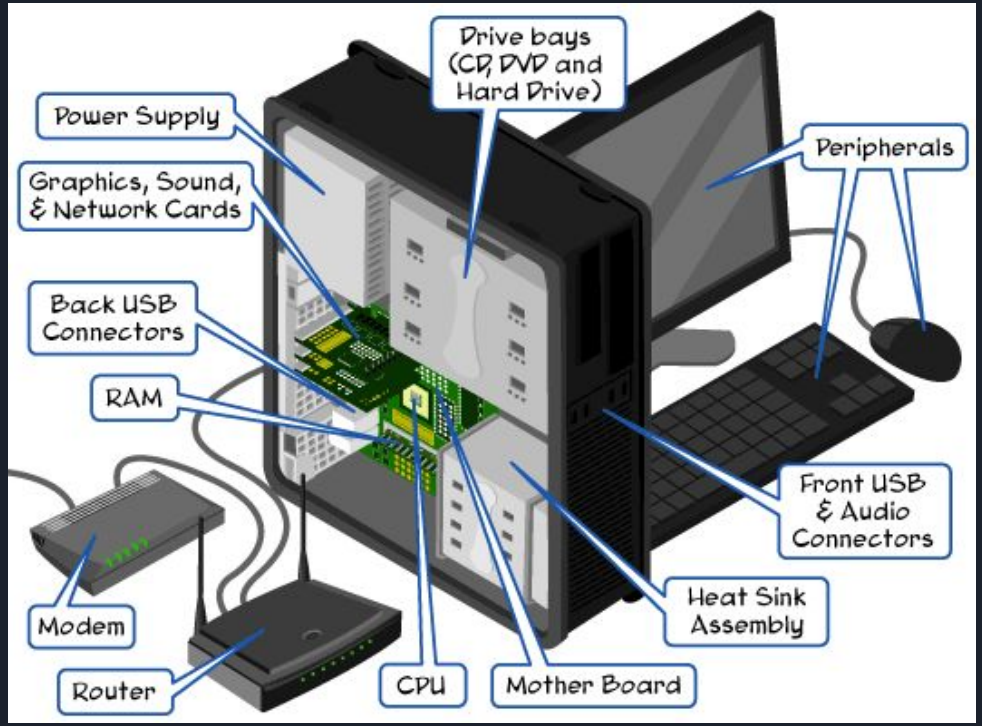
Entry Point

Host Forensics

Created by:
James Wernicke | wernicke@lanl.gov | @jwernicke
Shannon Beck | shannon@lanl.gov
Aaron Scott Pope | apope@lanl.gov

Introduction to Host Forensics

- Understand basic operating system anatomy
- Live system analysis
- Collect forensically sound evidence
- Static memory image analysis



Chain of Custody[§]

- Chain of evidence / chain of custody
  - Has to be maintained and documented correctly for court-admissible evidence
- [§]Please contact your local legal team for recommendations and procedures for your institution or company

Locard's Exchange Principle

Holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.

- Fingerprints
- Hair
- Digital traces
  - Shell history
  - Master File Table entries
  - Network traffic
  - Registry

Order of Volatility

What happens to your data when:

- Your computer is suddenly turned off?
  - Can you lose information?
- When you reboot, does your computer know:
  - What programs were running?
  - What files were open?

Forensic evidence collection needs to be prioritized by volatility

Cache

Cache memory is more temporary (volatile) than regular RAM memory

Sits with the CPU

Lost if the system is powered down

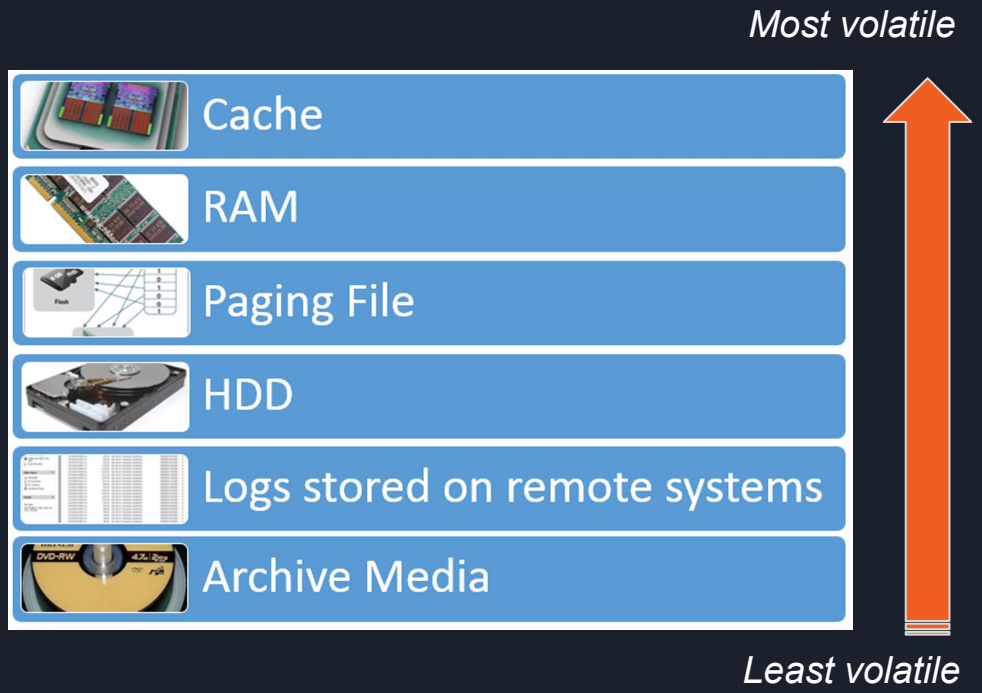


Image http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/

Random Access Memory (RAM)

Slightly less volatile than cache memory

Can include system and network processes information

Lost if the system is powered down

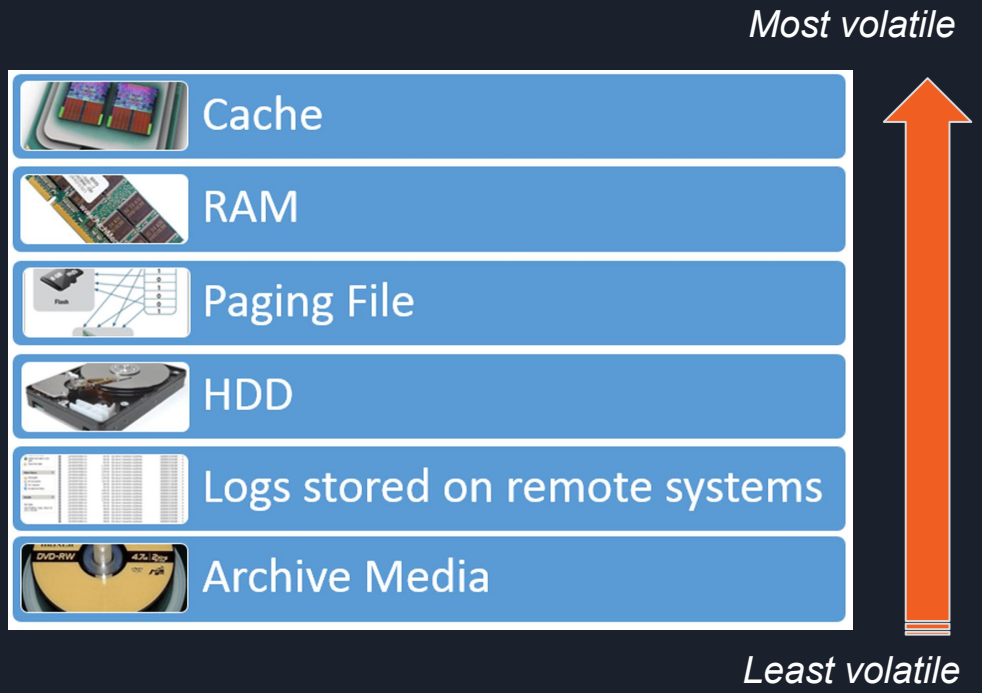


Image http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/

Paging File

An extension of RAM, but stored on the hard drive (HDD)

Paging file

- Rebuilt on reboot
- More volatile than "regular" HDD data

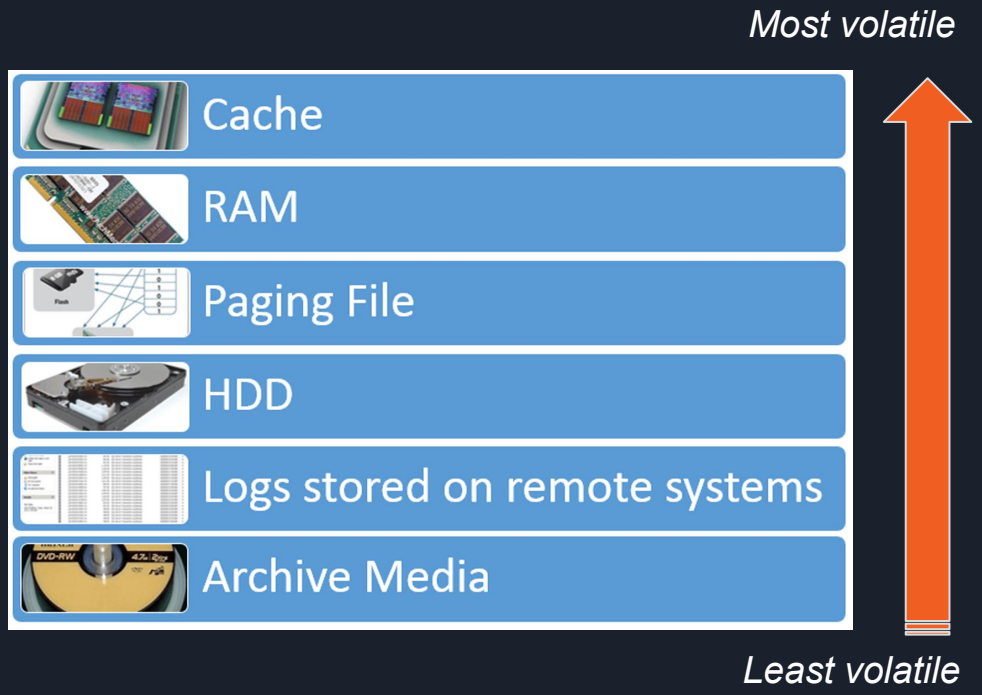


Image http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/

Hard Disk Drive (HDD)

Data stored on a hard disk drive (HDD) is semi-permanent

Remains on the hard drive without power / rebooted

Collect the *disk image* versus the *memory image*

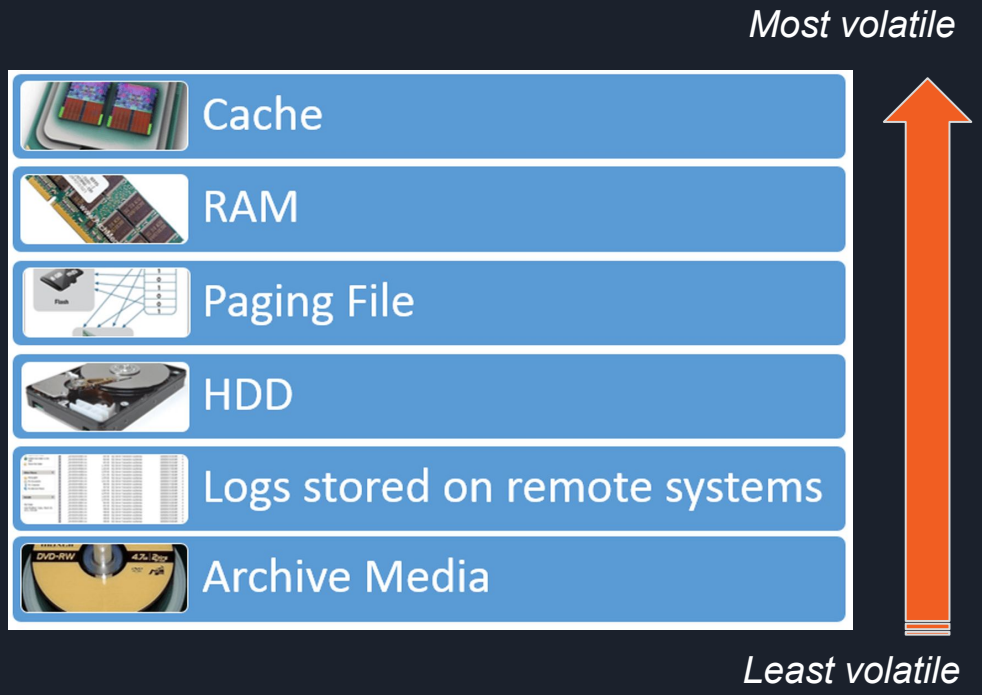


Image http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/

Logs

Your friend!

Any data stored on a remote system is less volatile than data stored on the target system.

Send log data to remote system for:

- Centralized collection and view
- Less volatility
- Searchable (Splunk)

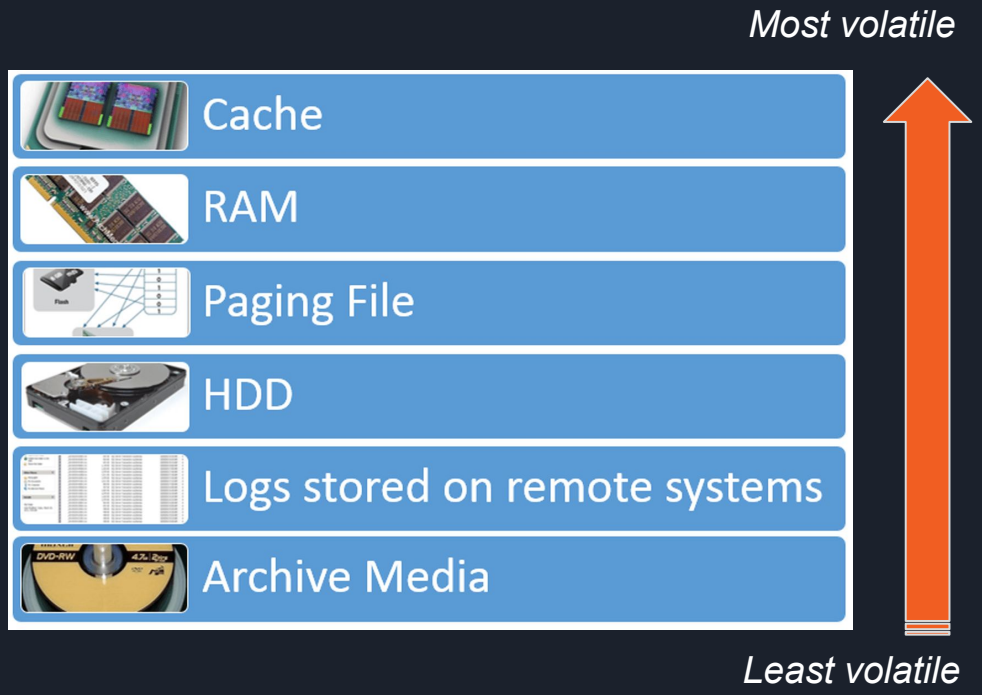


Image http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/

Archive / External Media

Backups / copies for recovery or archive purposes

Generally offline and less likely to be destroyed or corrupted

- Backup tapes
- DVDs
- USBs
- External Drives (tape, USB, cloud, other)

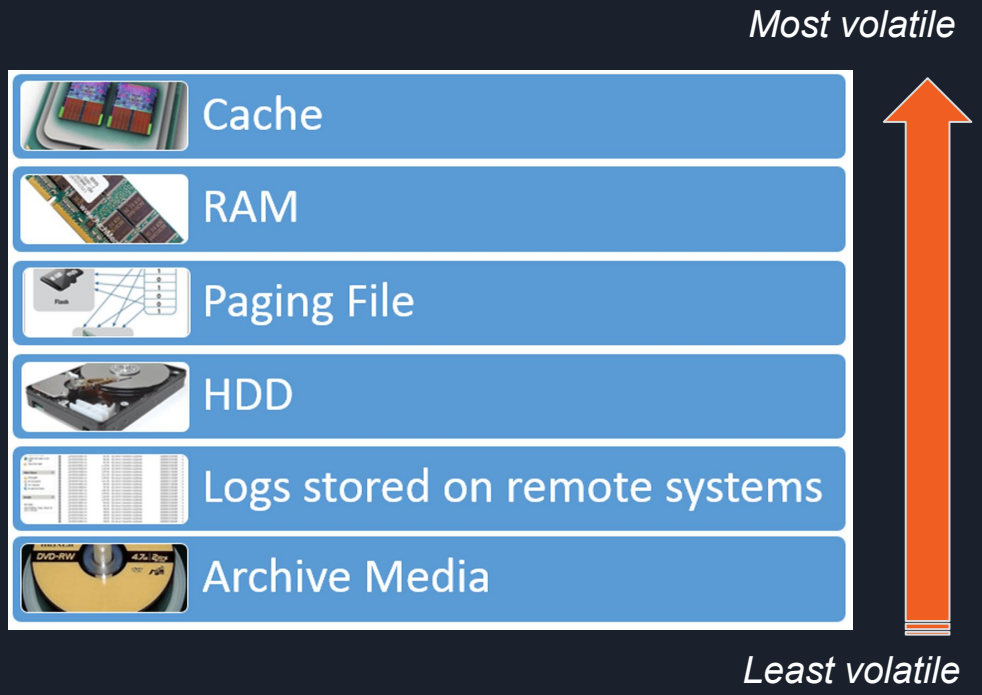


Image http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/

Volatile Forensic Data Collection

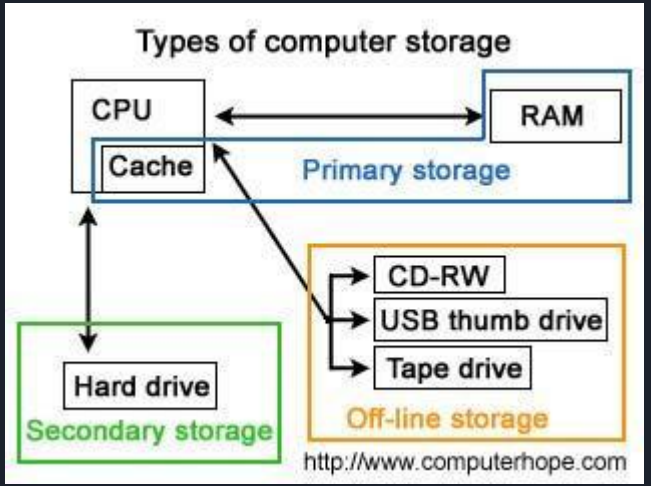
Don’t just turn off computer if it's suspected something is wrong

Before shutdown, collect what does not persist between reboots:

- Cache
- Memory
- Paging File

What is memory?

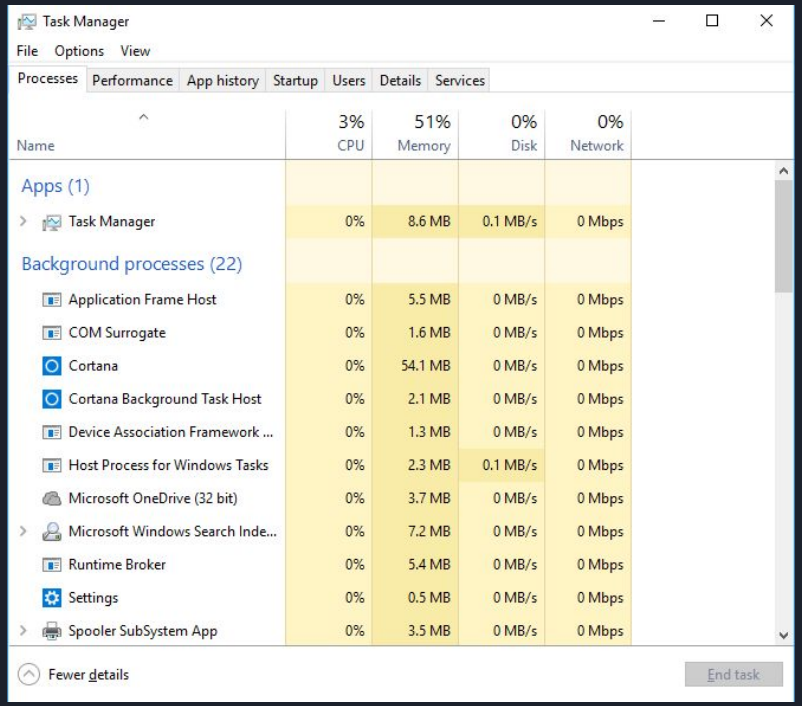
Computers use random access memory (RAM) to store recently used programs and data because it is many times faster to read and write data to RAM than hard drives and other types of storage. Today's computers commonly have 16GB or more of RAM which can store a LOT of data and programs. However, RAM is volatile memory so it loses any data stored in it when the computer is shut down.



Live System Analysis

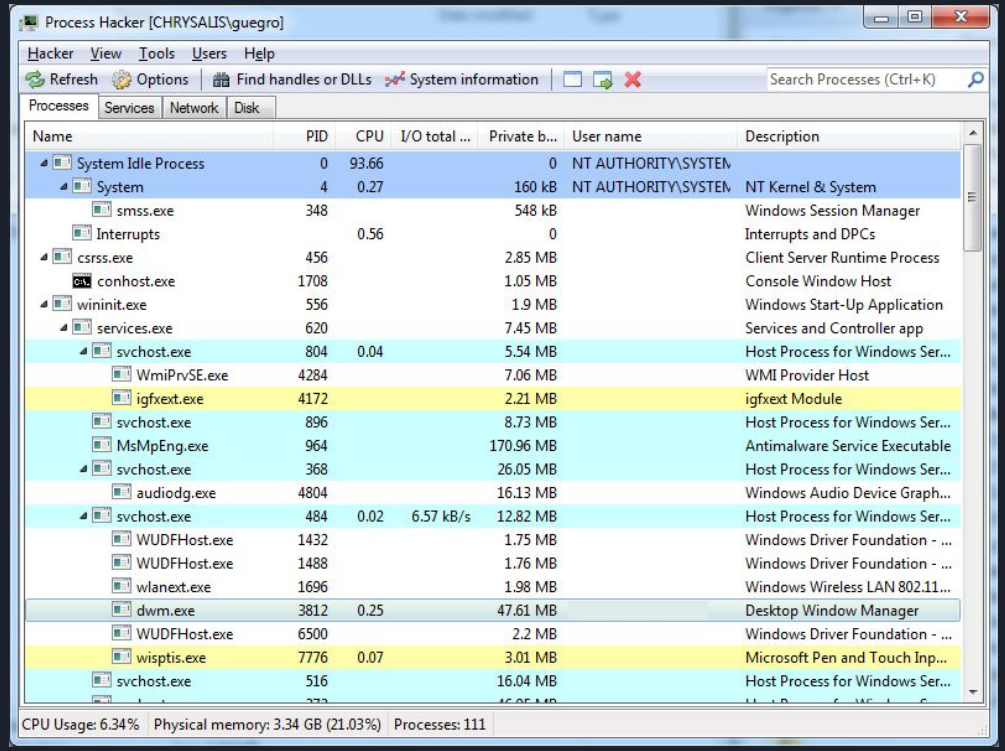
What is a process?

A process is an executing program. An application can consists of multiple processes. Processes are run by a user and inherit that user's privileges. Processes can read and write data as well as execute code. They can also spawn new processes, forming process trees. They often use built-in code libraries called dynamic link libraries (DLLs) that perform common functions without having to "reinvent the wheel".



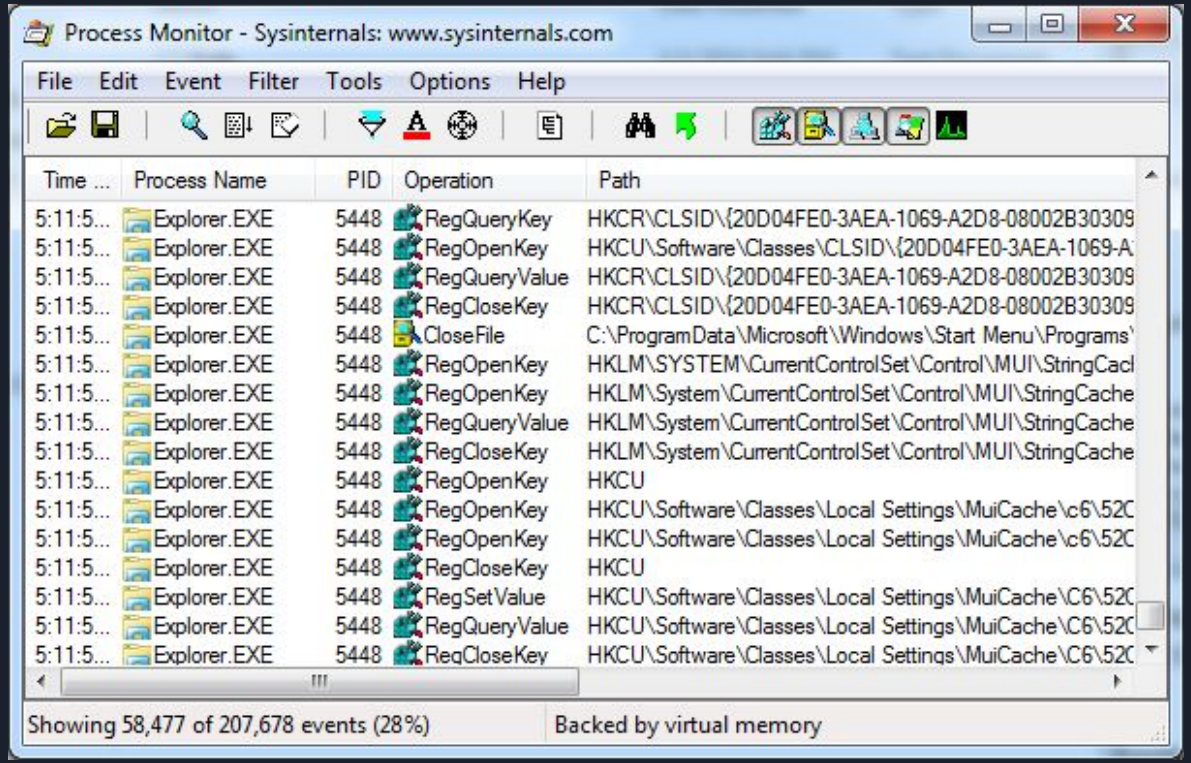
Process Hacker

Process Hacker is a free, open-source system monitor. It can be used to view what's going on in memory, such as currently running processes, network connections, and open files.

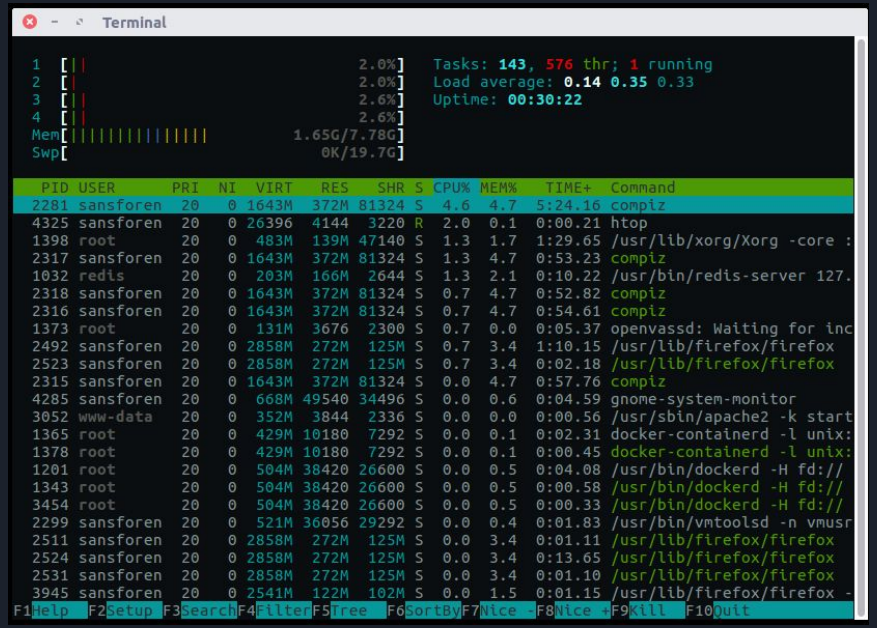


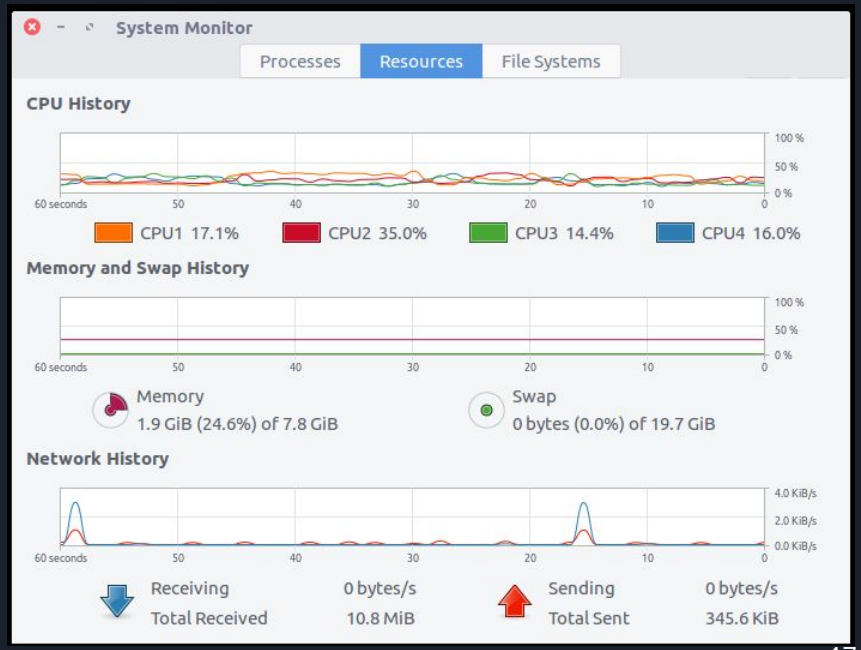
Process Monitor

Process Monitor is a real-time Windows monitoring tool. You can use it to watch what running processes are doing.



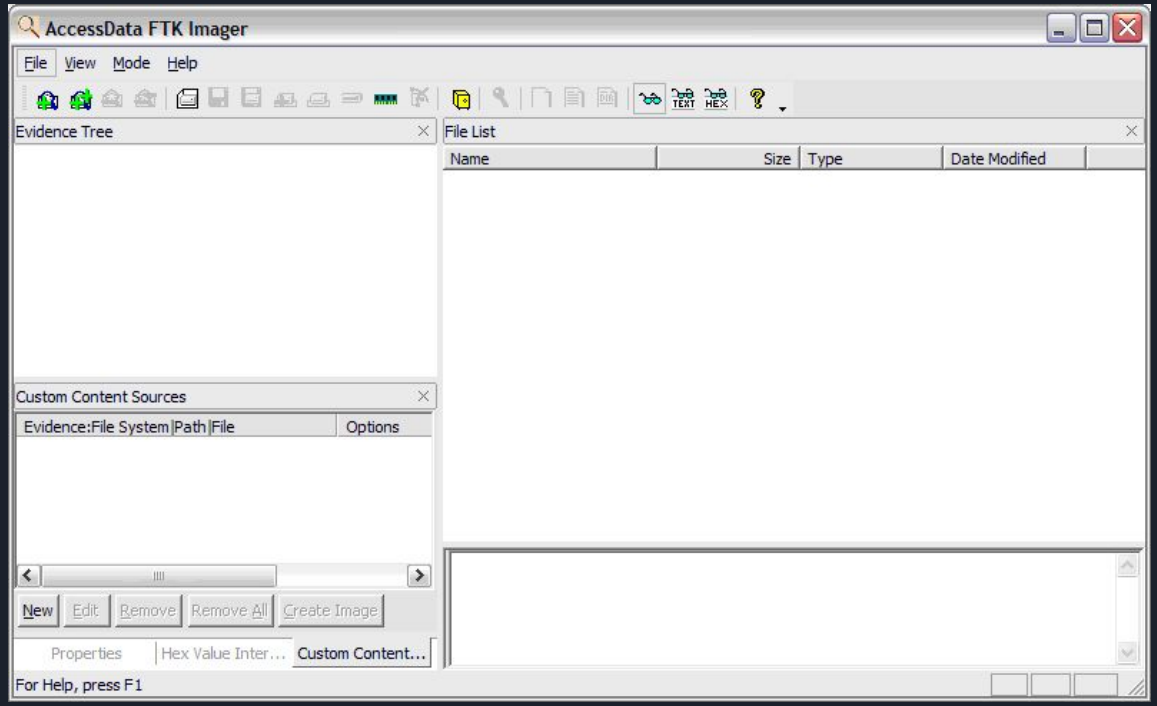
Live Linux Analysis





Forensic Memory Image Collection

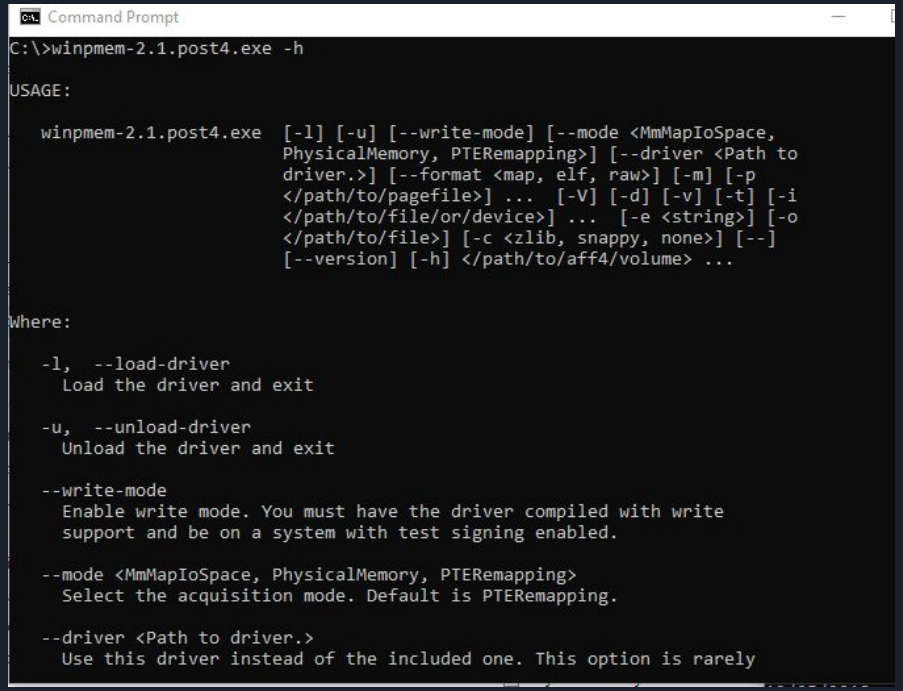
Graphical User Interface (GUI) tools available, such as FTK Imager by AccessData, for collecting the contents of memory on a running computer



Forensic Memory Image Collection

Command line tools, such as WinPmem, are more lightweight and less intrusive.

Pmem is an advanced, free, open-source memory collection tool. It is also quick, requires minimal memory, and can be run from a USB stick. Furthermore, it is compatible with some of the most popular memory analysis tools, including Rekall and Volatility.



Forensic Memory Image Analysis

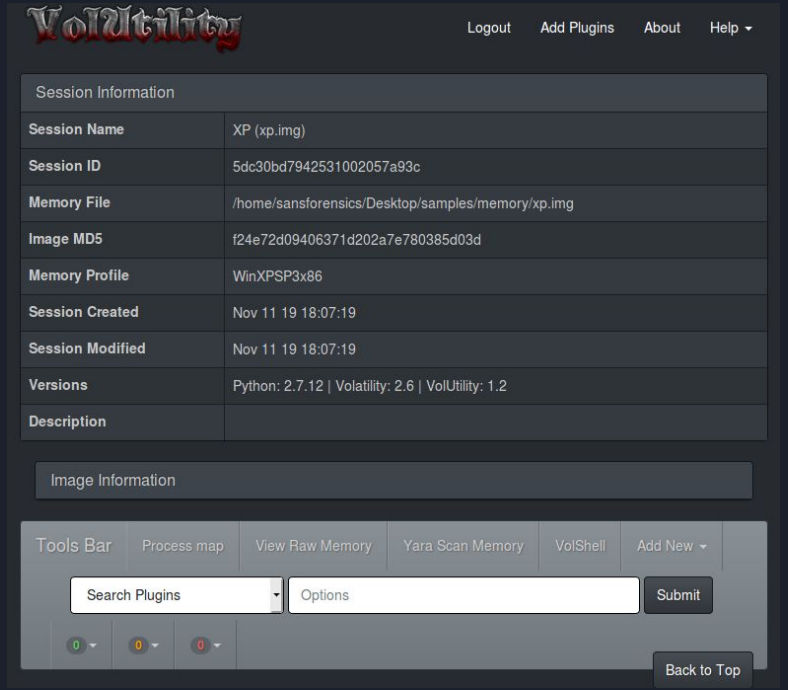
- Volatility is a command line tool for inspecting collected memory images
- Rekall is a similar spin-off project

```
$ vol.py --help
Volatility Foundation Volatility Framework 2.6
/usr/lib/python2.7/dist-packages/requests/__init__.py:83: RequestsDependencyWarning: Old
ersion of cryptography ([1, 2, 3]) may cause slowdown.
  warnings.warn(warning, RequestsDependencyWarning)
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/home/sansforensics/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
```

Forensic Memory Image Analysis

- VolUtility is a web-based graphical user interface (GUI) for working with Volatility
- Results are stored in a database to avoid repeated runs
- Results can be viewed through the web interface or exported for documentation



Exercise Time

Puzzle category:

- HostForensics

If you get bored:

- IntroToProgramming

Entry Point

Forensic Disk Imaging

Created by Shannon Beck | shannon@lanl.gov

Forensic Disk Image Analysis

- Disk image: a snapshot of a hard drive at a given point in time
  - Files
    - Emails
    - Calendar entries
    - Documents
    - Spreadsheets
    - Pictures
    - Malware
  - Cache files from web browsers
  - Master File Table
    - Information about current and deleted files
  - System registries

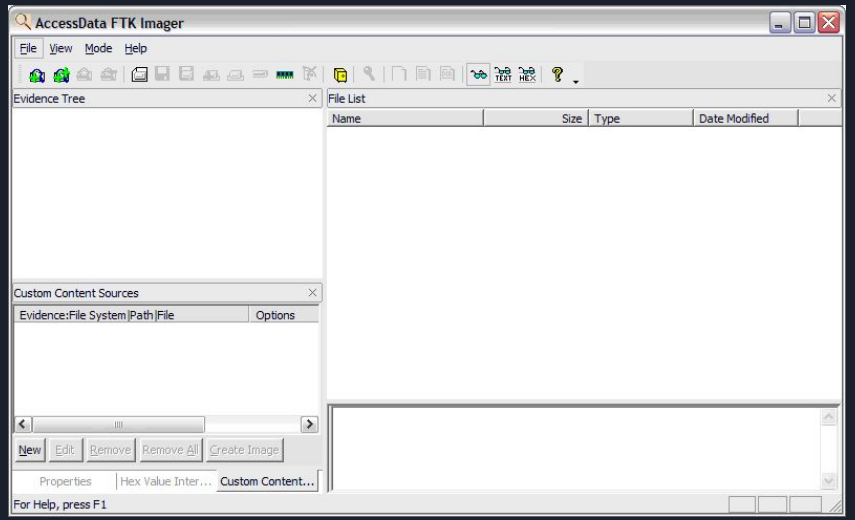
Forensic Disk Image Collection

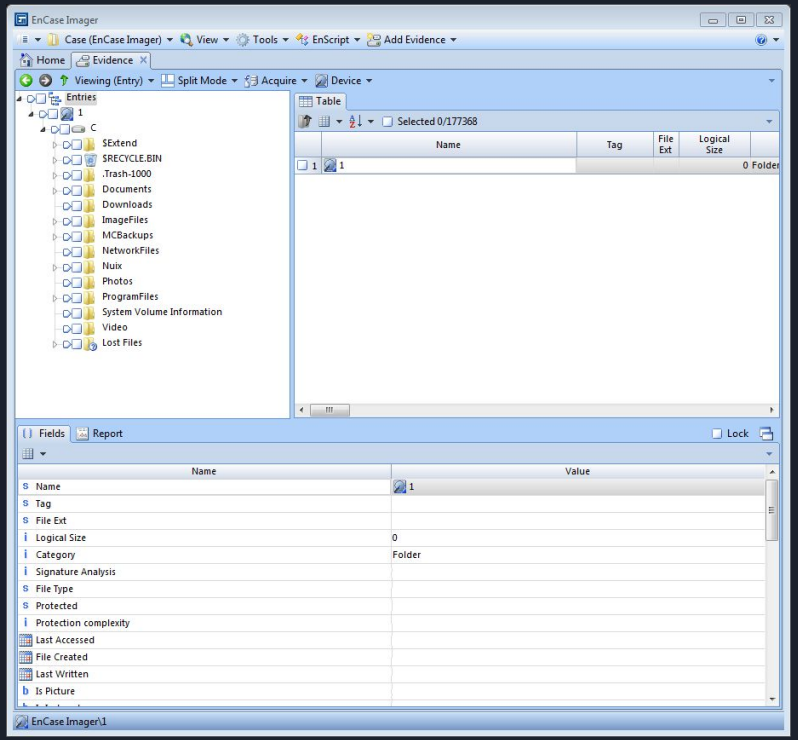
Dedicated hardware solutions

- Disk cloning
- Disk-to-file
  - Raw
  - E01
  - DMG

Forensic Disk Image Collection: Windows

- EnCase
- FTK Imager





FTK Imager Lite

- Computer forensic software
- Court-cited disk imaging program
  - Images obtained can be admissible in court
  - Chain of custody and proper procedure
    - Talk to your lawyer, need a write blocker
- Make disk and memory image files
- View evidence disks and image files
- Analyze image and memory files
- Lite is the free version of FTK Imager

More About FTK Imager

- Saves images in multiple formats including
  - .e01, .dd, and RAW
- Recover deleted files
  - Also called file carving, covered in future topic
- Obtain live Windows registry files

Forensic Disk Image Collection: Linux

Raw imaging using dd command

```
root@siftworkstation -> ~
$ dd if=/dev/sdb conv=noerror,sync bs=128K of=./disk.img
816+0 records in
816+0 records out
106954752 bytes (107 MB, 102 MiB) copied, 0.46575 s, 230 MB/s
```

FTK Imager command line tool

```
root@siftworkstation -> ~
$ ./ftkimager --help
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon,
UT 84042
All rights reserved.

Usage:  ftkimager source [dest_file] [options]
```

Forensics File Formats

- Raw (dd): bit-by-bit copy, no compression or error checking
- Expert Witness Format (ewf): redundant integrity checking
- EnCase's Evidence File (.E01) Compressible, searchable
- Advanced Forensics Format (AFF): compressible, extensible, open source format
- Access Data (AD1): logical format doesn't capture slack space

Exercise Time

Puzzle category:

- ForensicDiskImaging

Entry Point

Network Layers

Created by Neale Pickett | neale@lanl.gov
and Aaron Pope | apope@lanl.gov

Computer Network Communications

- Communication happens in chunks known as “packets”
- Packets are layered
- Imagine sending a letter in an envelope, inside another envelope, ...
- Each “envelope” has information about what to do with the contents

Computer Addresses

- Computers have multiple addresses for different purposes:
  - Hardware address
  - Internet address
  - Local network address
  - Domain name
  - Port (application)

Hardware Address

Media Access Control (MAC) Address

- Example: a0-b1-c2-d3-e4-f5
- Associated with the network interface
  - A computer can have multiple
- Typically permanent, but can be changed
- MAC address can often be used to identify the make and model of the interface

Internet Address

Internet Protocol (IP) Address

- Example: 172.217.0.46 (IPv4)
- Most addresses are public (internet-wide)
- Some are reserved for private networks
- IPv4 addresses are running out
- IPv6 to the rescue!
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Communication Ports

- Lets a computer maintain multiple connections without getting confused
- 0-65535 (2^{16}-1)
- 0-1023 are reserved for privileged services
  - 22, 23 : Remote shell access
  - 80 : HTTP (websites)
  - 443 : HTTPS (secure websites)
- Higher ports (1024+) are often randomly generated

TCP/IP Layers

MAIL TRUCK

TO: TEXAS

TO: DALLAS

TO: ALICE

Ethernet
To: Alice's computer

IPv4
To: Alice's router

TCP
To: browser

HTTP
spud.jpg

TCP/IP Layers

Ethernet
To: Alice's computer
From: Alice's router

IPv4
To: Alice's router
From: akamai computer 3928

TCP
To: browser
From: a web server

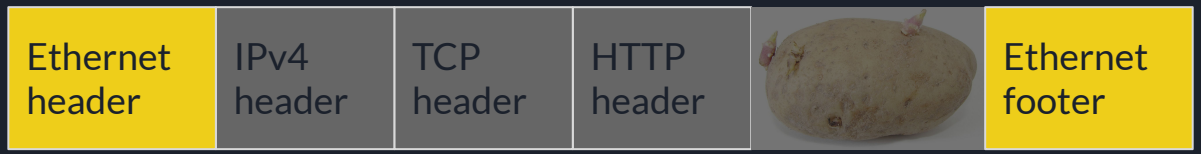
HTTP
spud.jpg

Link Layer	*Network Interface*
Internet Layer	*Router*
Transport Layer	*Operating System*
Application Layer	*Web Browser*

Link Layer: Ethernet

Ethernet is what your wireless or wired network interface speaks. It has enough information to be able to talk to neighbors on the same Local Area Network (LAN). Ethernet contains:

- Who's speaking (source MAC address)
- Who this is to (destination MAC address)
- What type of stuff is inside
- How big that stuff is



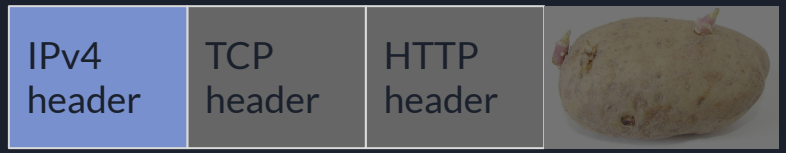
Link Layer

Network Interface

Internet Layer: IPv4 or IPv6

Your *router* works at the Internet layer, and delivers packets to other routers all over the world. To do this, it specifies:

- Who's speaking (source IP address)
- Who this is to (destination IP address)
- What type of stuff is inside



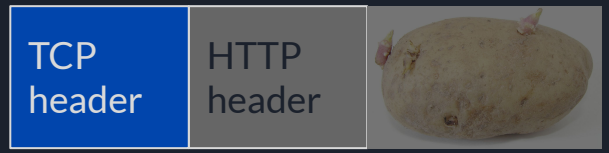
Internet Layer

Router

Transport Layer: TCP or UDP

Once a packet has arrived on your computer, the Operating System looks at the transport layer to figure out which program should get the next layer. The transport layer has:

- Who's speaking (source port)
- Who this is to (destination port)
- What type of stuff is inside



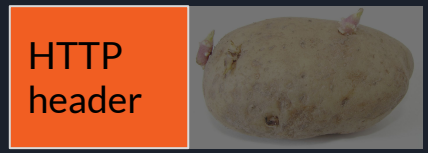
Transport Layer

Operating System

Application Layer: HTTP or SMTP

We're almost there! The application layer could have anything in it: that's up to the application. It could have an email, a movement event for a game, a video frame, or anything else. In our example, it has an HTTP message containing an image.

Since the transport layer had a value corresponding with the web browser in our operating system, the browser gets this message, interprets the HTTP header, and passes the rest on to the imaging routines.



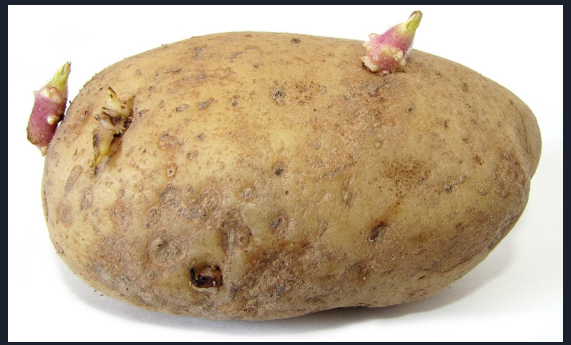
Application Layer — *Web Browser*

Potato Layer?

TCP/IP doesn't specify what happens inside the application layer.

Since this was HTTP, we need to read the HTTP specifications to figure out how to handle the rest of the stuff. We're going to just call it the Potato Layer for now.

Network Archaeology dives deep into the potato layer!



Exercise Time

Puzzle category:

- NetworkLayers

If you get bored:

- NetworkFundamentals
- PortsandProtocols
- IPandSubnetting

Entry Point

Networking - Routing

Created by Neale Pickett | neale@lanl.gov
and Aaron Pope | apope@lanl.gov

Computer Addresses Reminder

- Hardware address
  - MAC: a0-b1-c2-d3-e4-f5
- Internet address
  - IPv4: 172.217.0.46
  - IPv6: 2001:0db8:85a3::8a2e:0370:7334
- Application
  - Port: 80

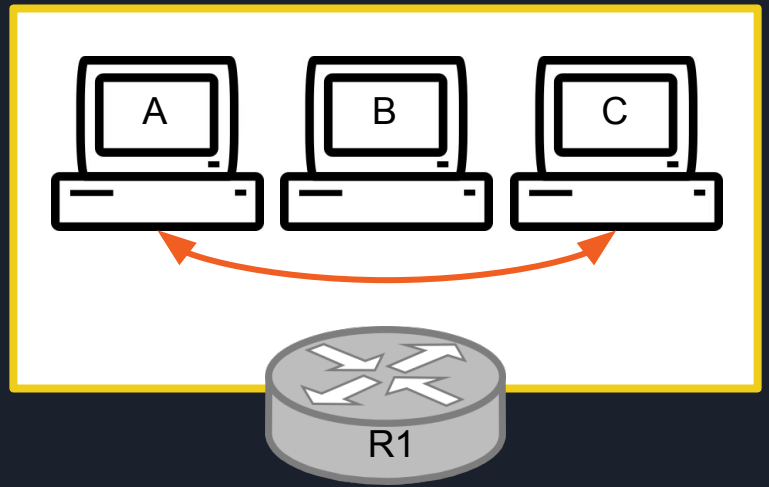
IP Addresses and Subnets

- A *subnet* is a group of machines that can talk to each other without a router.
- Subnets can be different sizes, and are defined by a *netmask*.
- Netmasks are usually specified by *CIDR notation*: the number of bits that specify the subnet.

192.168.27.12/32	1 IP	192.168.27.12
192.168.27.0/24	256 IPs	192.168.27.0 - 192.168.27.255
192.168.0.0/16	65k IPs	192.168.0.0 - 192.168.255.255
192.0.0.0/8	16m IPs	192.0.0.0 - 192.255.255.255

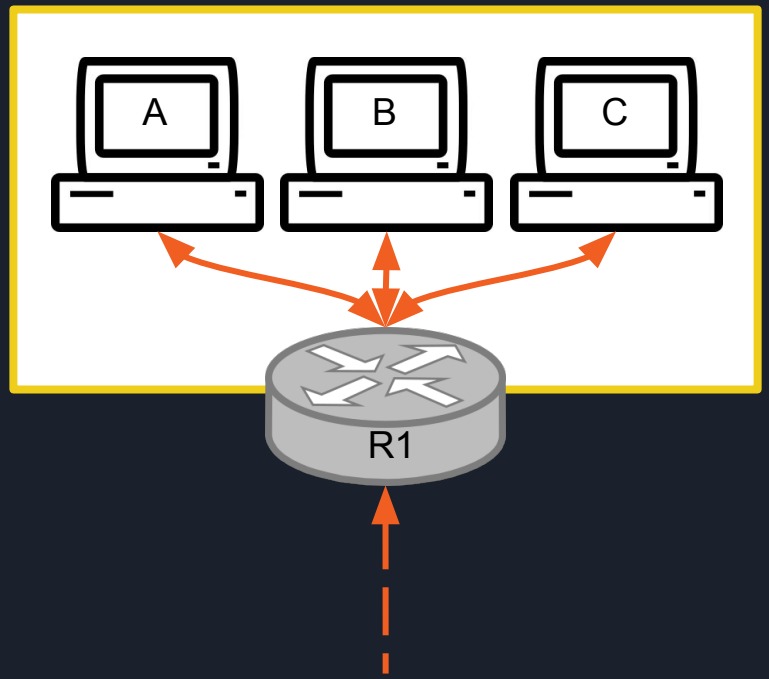
Network Routing

- Computers A, B, and C are on the same subnet
- They can communicate directly with each other without relying on the router R1



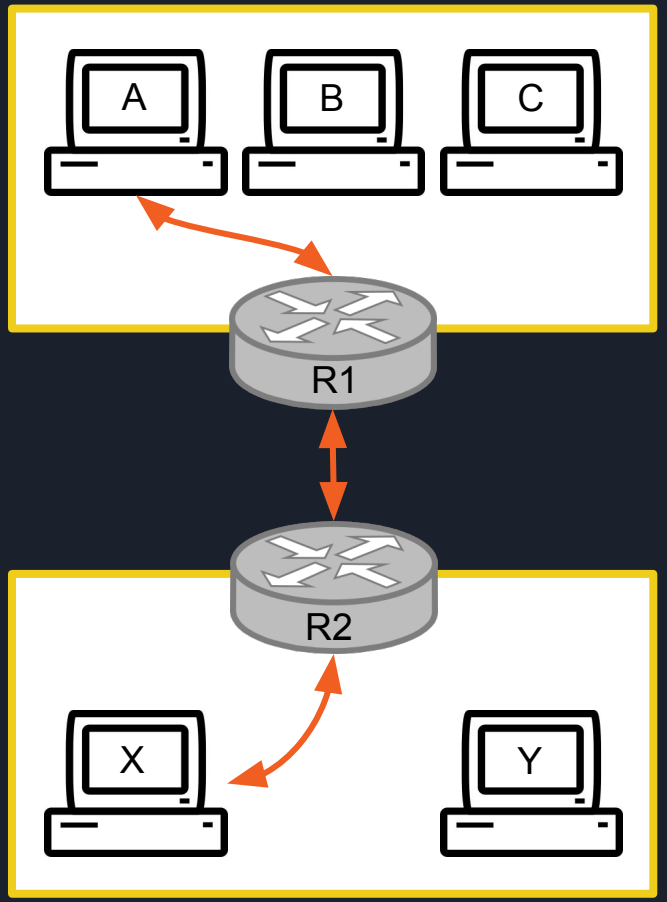
Network Routing

R1 serves as the *gateway* for A, B, and C, providing a path to everything outside of their subnet



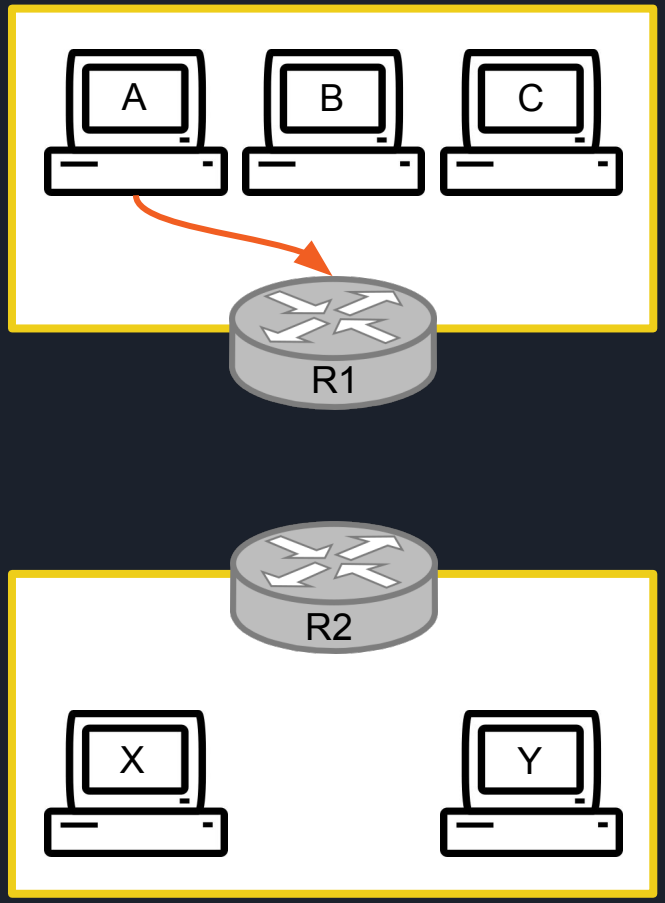
Network Routing

- Computers X and Y are in a different subnet
- Communication between A and X must go through routers, which connect subnets



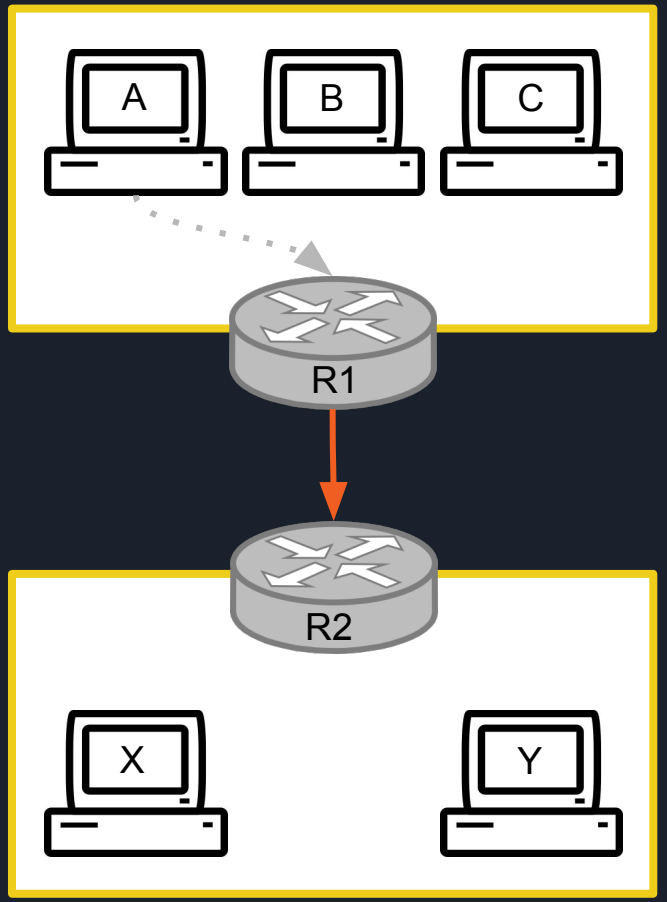
Network Routing

To send a message to X, A addresses the message with X's internet address but R1's hardware address



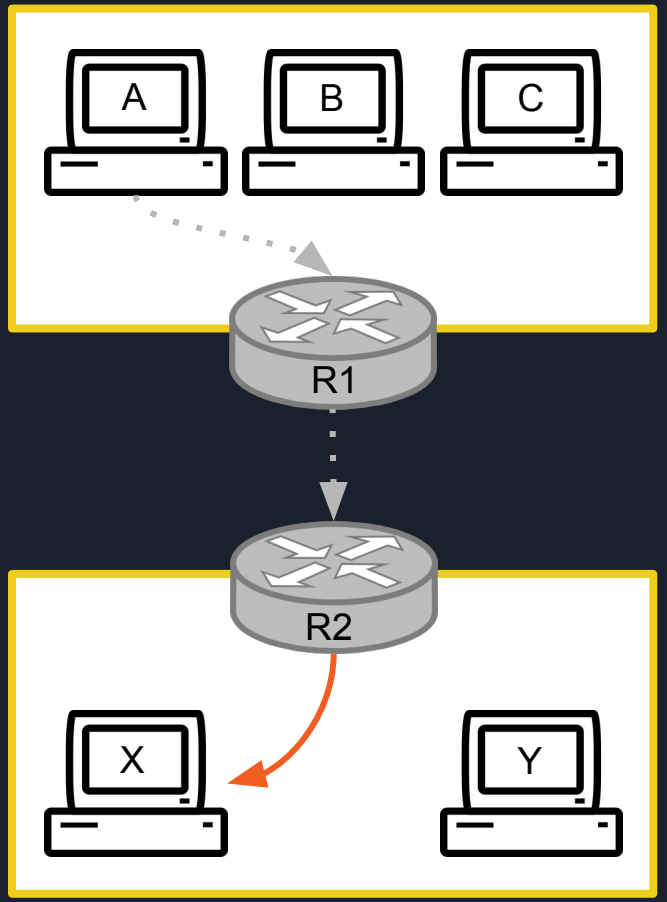
Network Routing

Then, R1 uses X's internet address to determine that it needs to forward the message to R2



Network Routing

Finally, R2 sends the message addressed to X's hardware address



Exercise Time

Puzzle category:

- NetworkRouting

If you get bored:

- NetworkFundamentals
- PortsandProtocols
- IPandSubnetting

Entry Point

Packet Capture

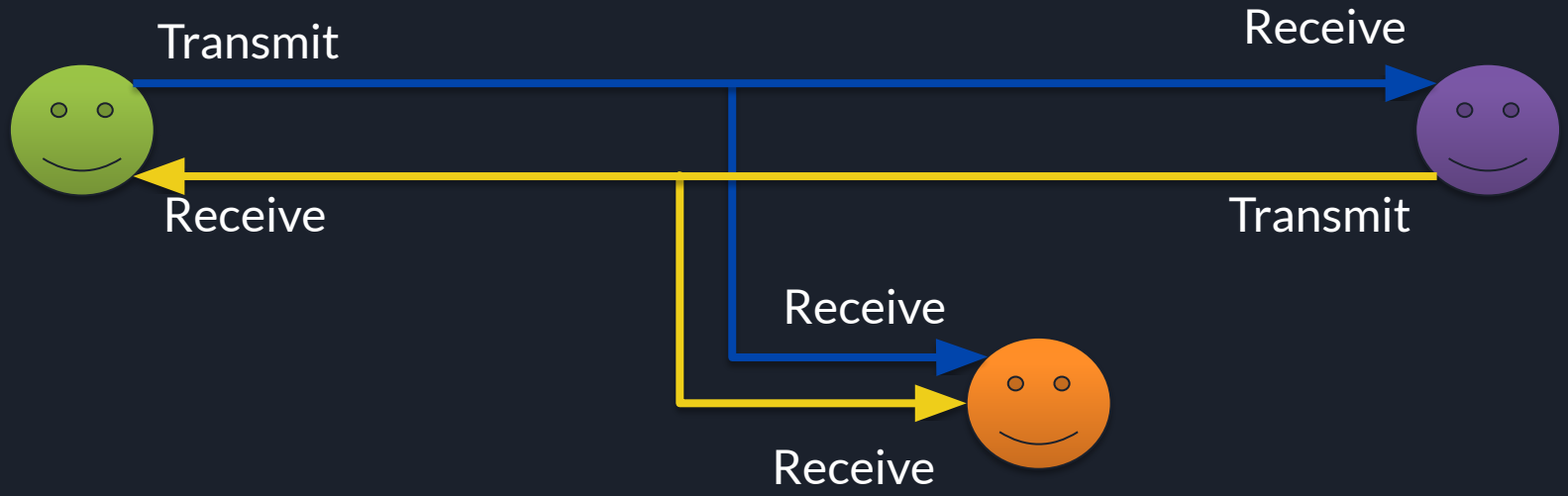
Created by Neale Pickett | neale@lanl.gov
and Aaron Pope | apope@lanl.gov

Observing Network Traffic

- Transmitting something over a network isn't like sending a physical package
- The intended recipient isn't the only one who can see the message
- Visible to any device on the network
- Generally, devices just ignore messages that aren't for them
- Network taps can observe all messages
- Packet capture: tracking packets seen by a tap
    - Often stored for later analysis

Wire Tapping 101

Wire Tapping 101

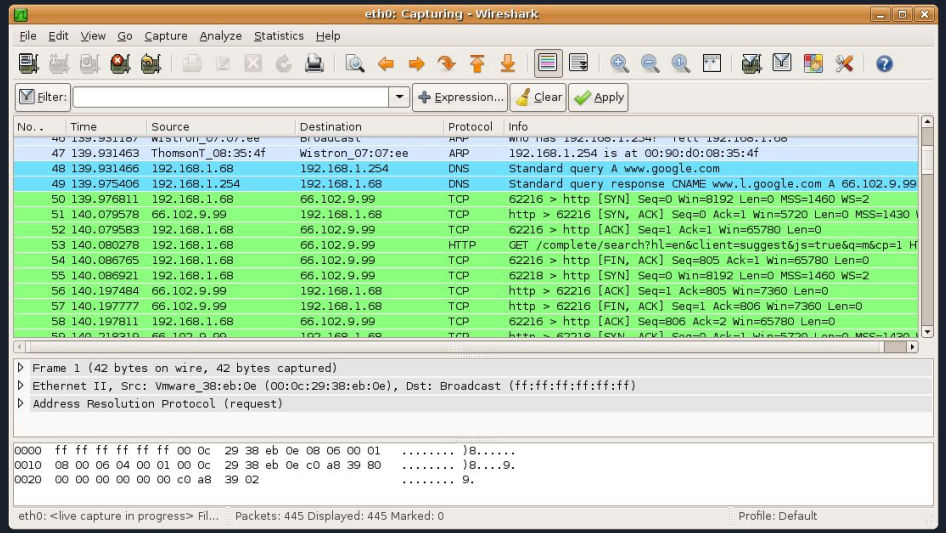


Wire Tapping 101: Tap Hardware

Many types of taps exist for various applications and media. But most taps are passive: they only listen.

Wire Tapping 101: Wireshark

- Wireshark packet analysis
- Can be used as a “software tap”
- Captures any traffic visible to your computer, including its own
- Store packet capture, or “PCAP” files
- Can be used to analyze PCAP files generated using other software or devices



eth0: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

eth0: <live capture in progress> Fil... | Packets: 445 Displayed: 445 Marked: 0 | Profile: Default

Wire Tapping 101: I have packets, now what?

Once you have a bi-directional flow of packets, you can:

- (Attempt) to decode any encoded messages (HTTPS)
- Reconstruct the exchange of information from the packets
  - Pictures
  - Software
  - Documents
  - Videos
  - Communication

Exercise Time

Puzzle category:

- PacketCapture

If you get bored:

- NetworkFundamentals
- PortsandProtocols
- IPandSubnetting

Entry Point

Networking - Protocols

Created by Neale Pickett | neale@lanl.gov
and Pablo Arias | arias13@llnl.gov

SMTP

- Simple Mail Transfer Protocol
  - Email
  - Has grown less simple over the years
- TCP Port 25
- Client and Server have a back-and-forth conversation
  - It turned out this is really slow over high-latency links
  - This style of protocol is hardly ever used anymore
- Spam wasn't invented until 1994
  - ISPs kept turning off ports to try and prevent it
  - Now only servers speak SMTP to each other

SMTP Example

```
220 WowzaMail Server 14.8
EHLO example.com
250 Hello, nice to meet you.
MAIL FROM: Neale Pickett <neale@example.com>
250 Sender OK
RCPT TO: Shannon Beck <shane@example.com>
250 Recipient OK
DATA
354 Enter mail, end with "." on a line by itself
From: Santa <hohoho@northpole.nl>
To: Timmy <hopalong@cratchit.name>
Subject: You've been a good boy

Dear Timmy,
```

HTTP and HTTPS

- HyperText Transfer Protocol (HTTP) sends HyperText Markup Language (HTML)
  - Links were originally “HyperLinks”, because that sounded cooler to somebody
  - Linking together two resources on different computers was a pretty wild idea in 1989
- TCP port 80
- HTTPS adds encryption
  - TCP port 443
  - The “S” is for “Secure”
- Client asks for something, server responds
  - Only incurs latency twice
- Due to port blocks, almost everything uses HTTPS now

HTTP Example

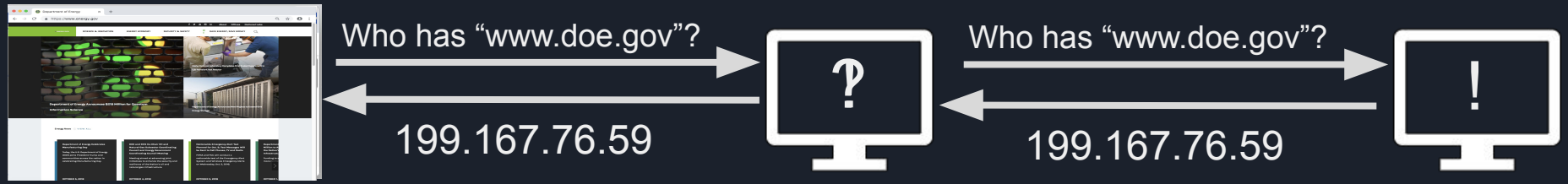
```
GET /potato.jpg HTTP/1.1
Host: example.com

HTTP/1.1 200 OK
Content-Type: image/jpeg
Content-Length: 42896

..JFIF..........................  …
```

Domain Name Service (DNS)

- Finds an IP address from a domain name (google.com)
  - Easier to remember domain names (such as DOE.gov) than to remember an IP address
- UDP Port 53
- Need to have DNS configured or internet will not work properly (to end user)
  - Common DNS Servers: 8.8.8.8, 1.1.1.1, ISP / Employer DNS Server
- Commonly unblocked port, since internet relies heavily on DNS



DNS Example

```
$ nslookup www.doe.gov

Server:       8.8.8.8
Address:      8.8.8.8#53

Non-authoritative answer:
www.doe.gov       canonical name = www.energy.gov.
www.energy.gov    canonical name = energy.gov.
Name:         energy.gov
Address: 199.167.76.59
```

Dynamic Host Configuration Protocol (DHCP)

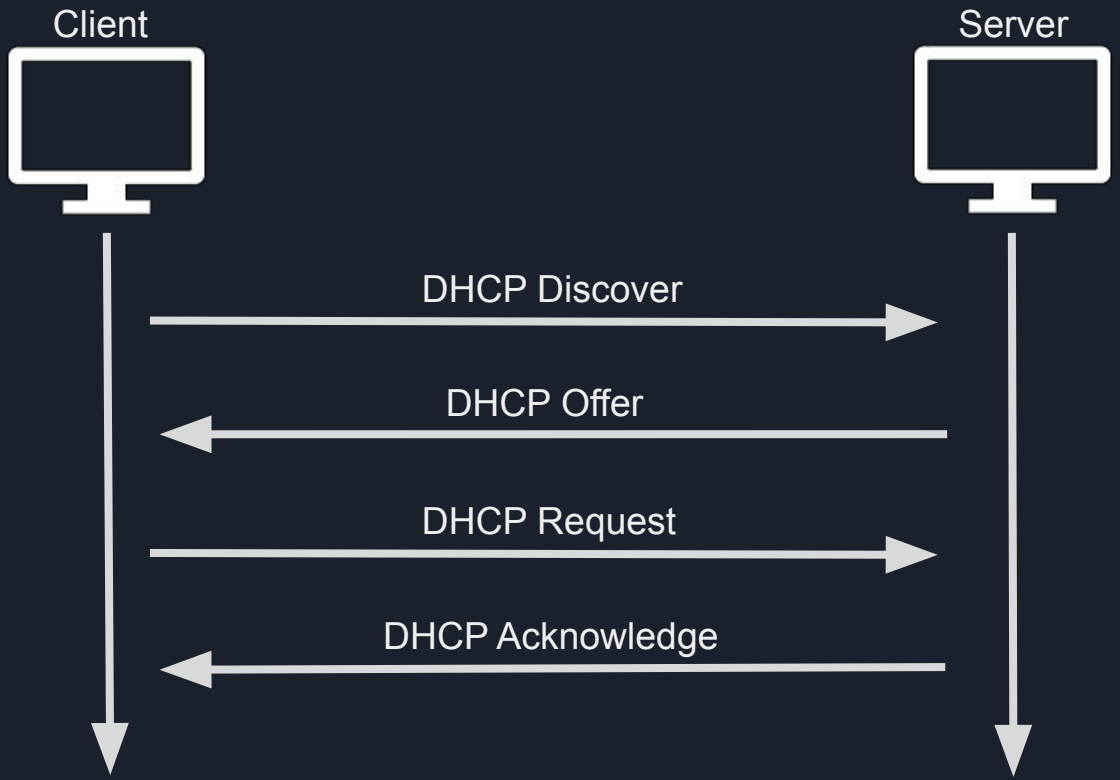
Assigns dynamic IP address on a network

- Allows network to dynamically assign and revoke IP addresses specified by the network administrator
- Each IP address will contain a lease time that indicates how long a client utilize IP (default is 8 days)
- Number of addresses depends on network configuration (remember subnetting)

Different from static IP addresses

- Static IP address is manually assigned and will not change
- Will need to let DHCP server know not to offer static IP address (DHCP Reservation)

DHCP Process



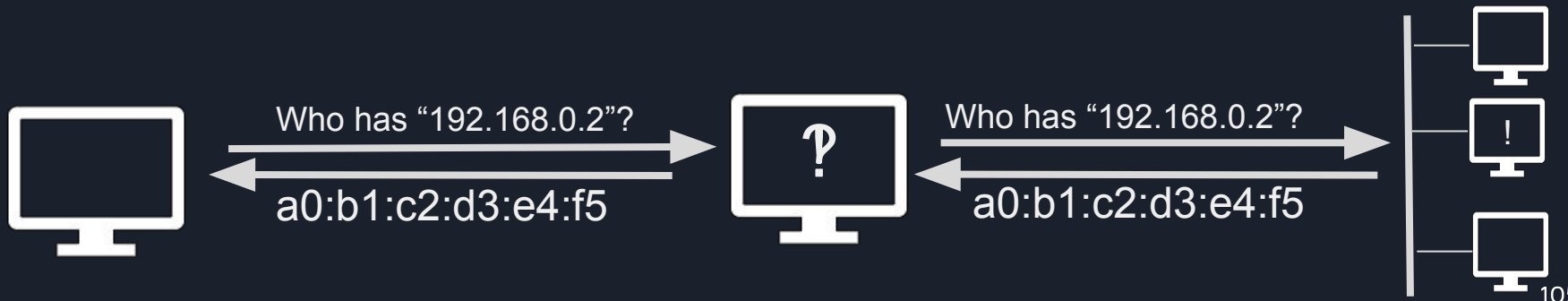
Address Resolution Protocol (ARP)

Gets a hardware (MAC) address for an IP

- Each device will contain a unique MAC address that is used to connect to a network
  - Devices may contain more than one MAC address. One for each Network Interface Card (NIC)
- Routers will utilize MAC address to send data between devices
  - ARP will allow the router to know where to route packets to/from each device via MAC address'
- Each device will contain ARP table to cache (store) results

ARP Process in a Local Area Network (LAN)

1. Packet will contain an IP address to which data will need to be sent to/from
2. System will consult ARP table
3. System will send broadcast “Who has IP 192.168.0.58” to everyone in the Local Area Network (LAN)
4. System with IP address “192.168.0.58” will respond with a MAC address.



Network Address Translation (NAT)

Maps one IP address space (like the Internet) to another (like your home network)

- IPv4 - 2^32 number of IP address' (roughly 4 billion addresses)

Using NAT, a router will allow a device to communicate to public IP address' using an internal private IP address

Reserved internal (private) IP addresses

  - 192.168.0.0/16
  - 10.0.0.0/8
  - 172.16.0.0/12

NAT: How to Assign A DHCP Address

One-to-One Mapping: Static & Dynamic

- Static: permanent mapping between an internal address to a specific public IP address
- Dynamic: mapping between of an internal address to a specific public IP address grabbed from a pool of addresses.

Internal IP	External IP
192.168.0.10	1.2.3.4
192.168.0.11	1.2.3.5

One-to-Many: Port Address Translation (PAT / Overloading)

- Most commonly used form of NAT
- Router will map an internal IP address to a specific port

Internal IP	External IP
192.168.0.10	1.2.3.4:9000

Exercise Time

Puzzle category:

- NetworkProtocols

If you get bored:

- NetworkFundamentals
- PortsandProtocols
- IPandSubnetting

Entry Point

Network Scanning

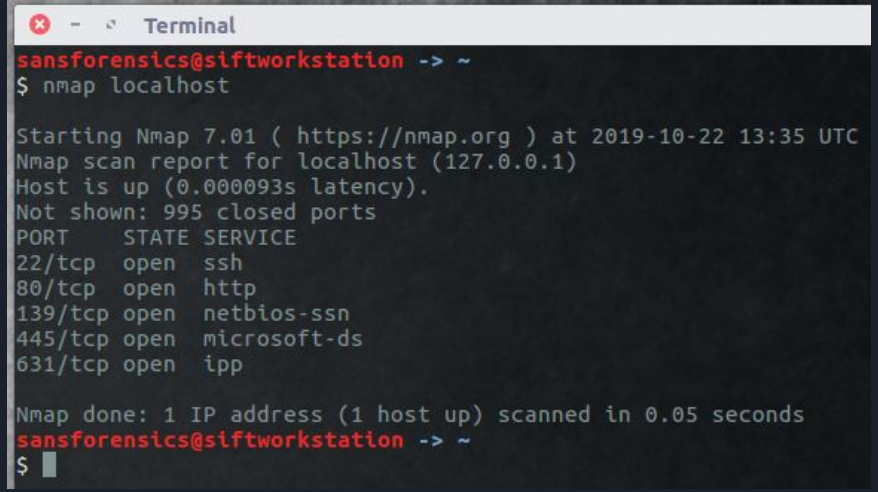
Created by Aaron Pope | apope@lanl.gov

Network Scanning

- Sometimes the evidence won't be enough to fully understand an incident
- Knowing how an intruder got in might require looking for network vulnerabilities
- Several automated tools to locate, understand, and mitigate security weak points

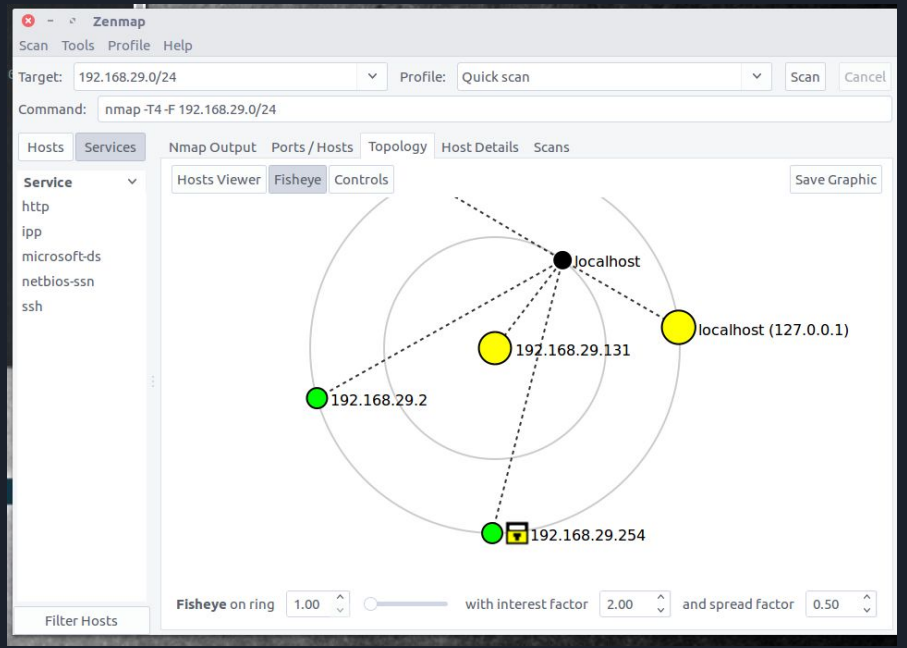
NMAP: Network Mapper

- Network host and service discovery tool
- Builds a “map” of the network
- Cross-platform



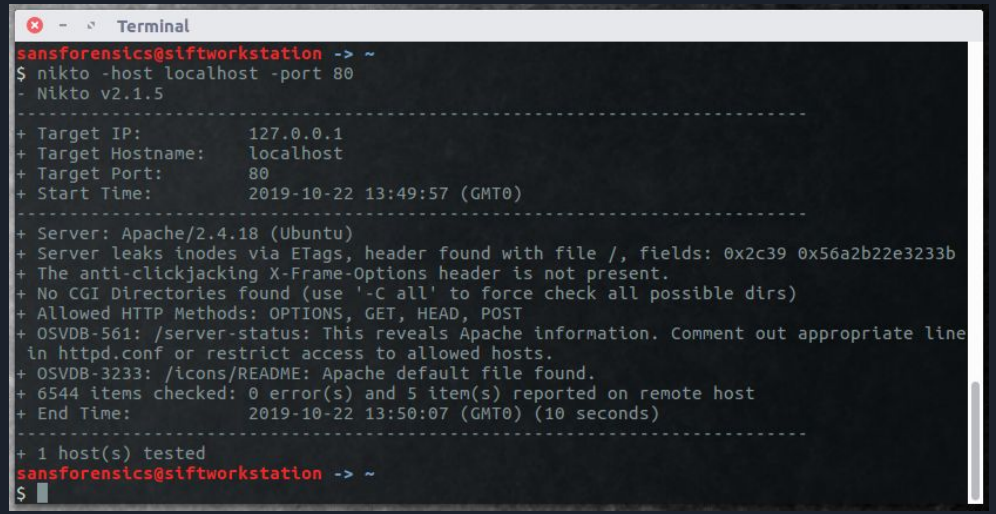
Zenmap

- GUI and visualizer for NMAP
- Has predefined scan “profiles”



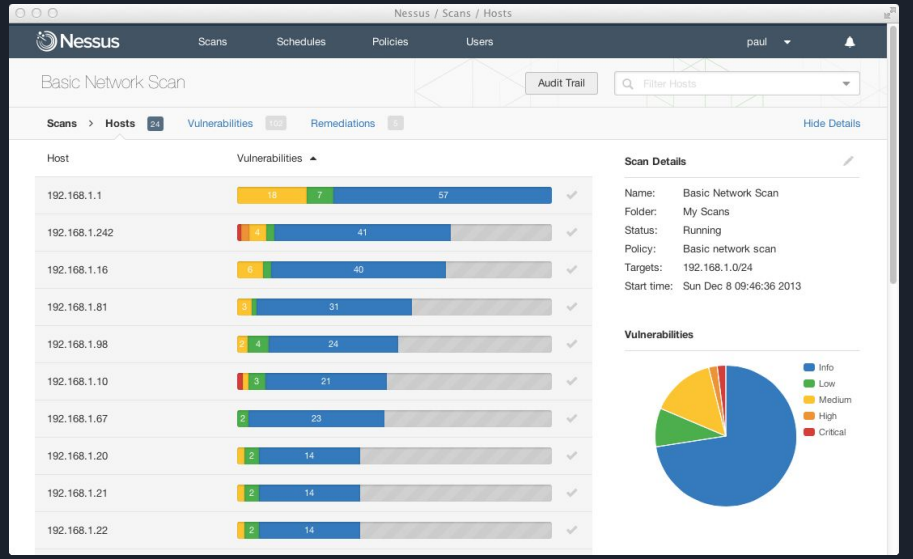
Nikto

- Command line vulnerability scanner
- Checks for unpatched services and misconfigurations



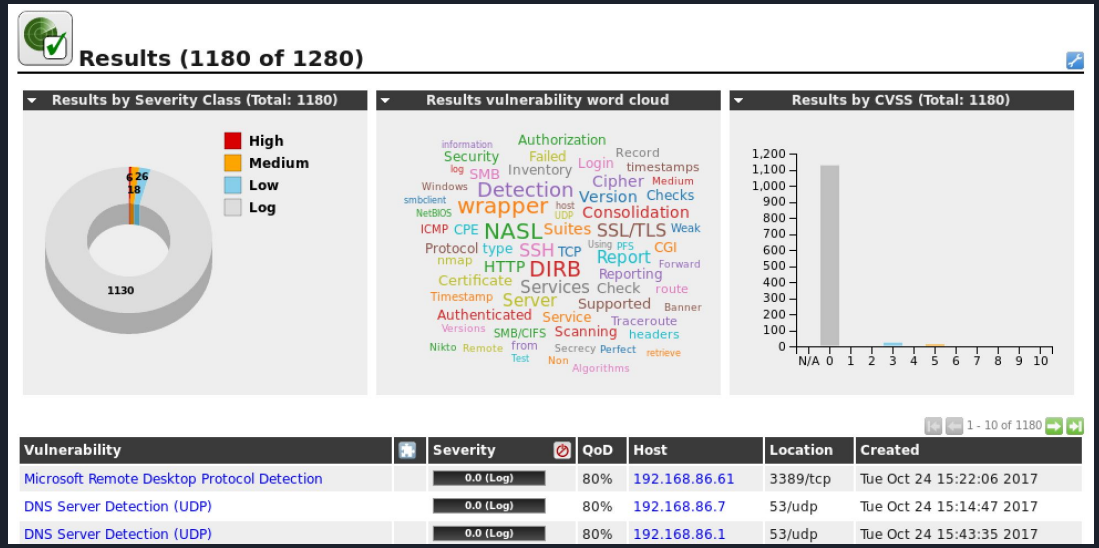
Nessus

- tenable.com/products/nessus
- Looks for security holes:
  - Misconfiguration
  - Default credentials
  - Unpatched services



OpenVAS

Open source alternative to Nessus



Exercise Time

Puzzle category:

- NetworkScanning

If you get bored:

- NetworkFundamentals
- PortsandProtocols
- IPandSubnetting

Entry Point

File Carving

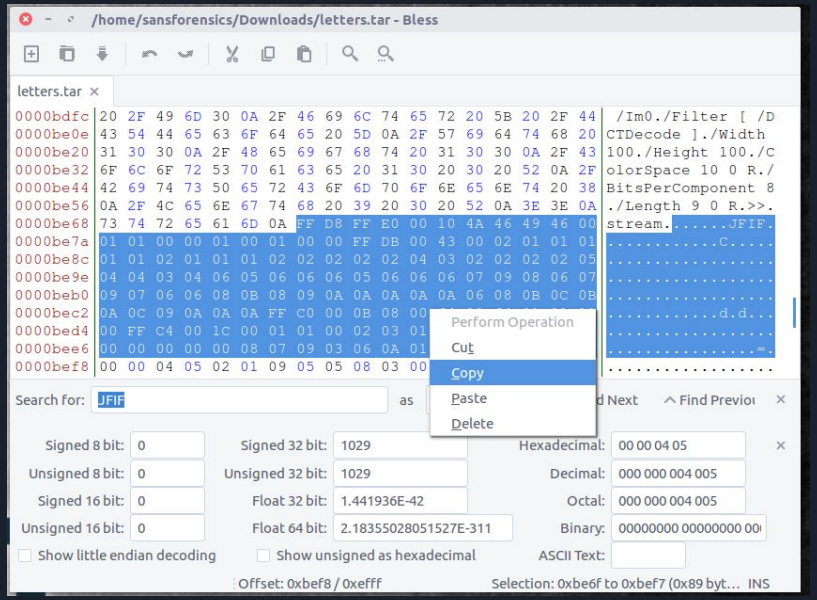
Created by Aaron Pope | apope@lanl.gov

File Carving

- Extracts file contents from raw information (e.g., memory or disk image)
- Relies on file signatures instead of OS file system management
- Allows recovery of deleted files, or files in formatted/unallocated space

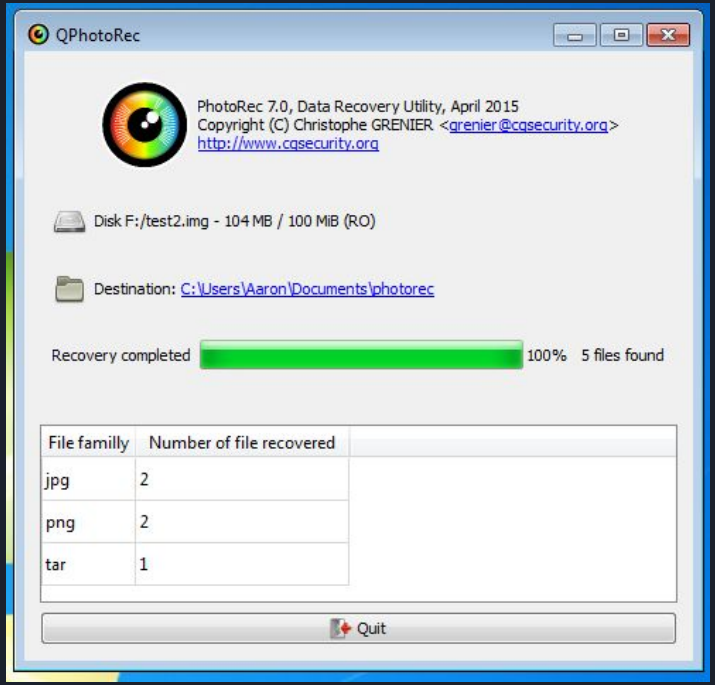
Manual File Carving

- Open raw information in hex editor
- Locate file beginning and end using file signatures
- Copy and paste into new file



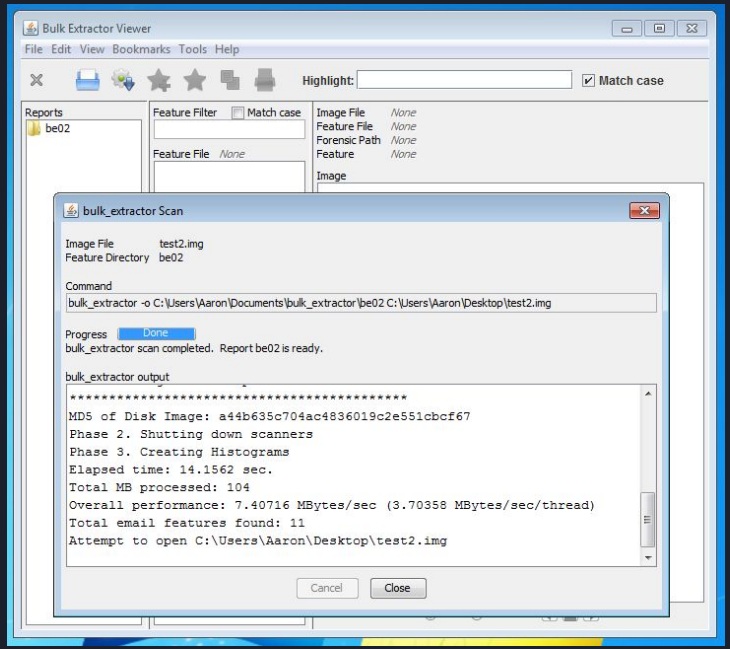
Automated File Carving

- Exhaustive search for known file signatures
- Finds hidden or deleted files
- Can reconstruct files
- Can be very slow for large drives



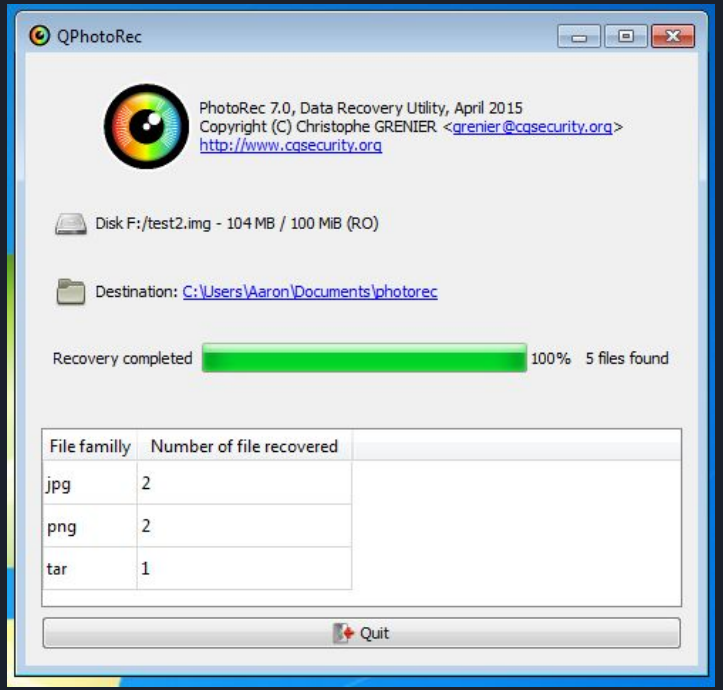
Bulk Extractor

- Forensics tool with some limited signature analysis and carving capability
- Only identifies contiguous JPEG, ZIP and RAR files



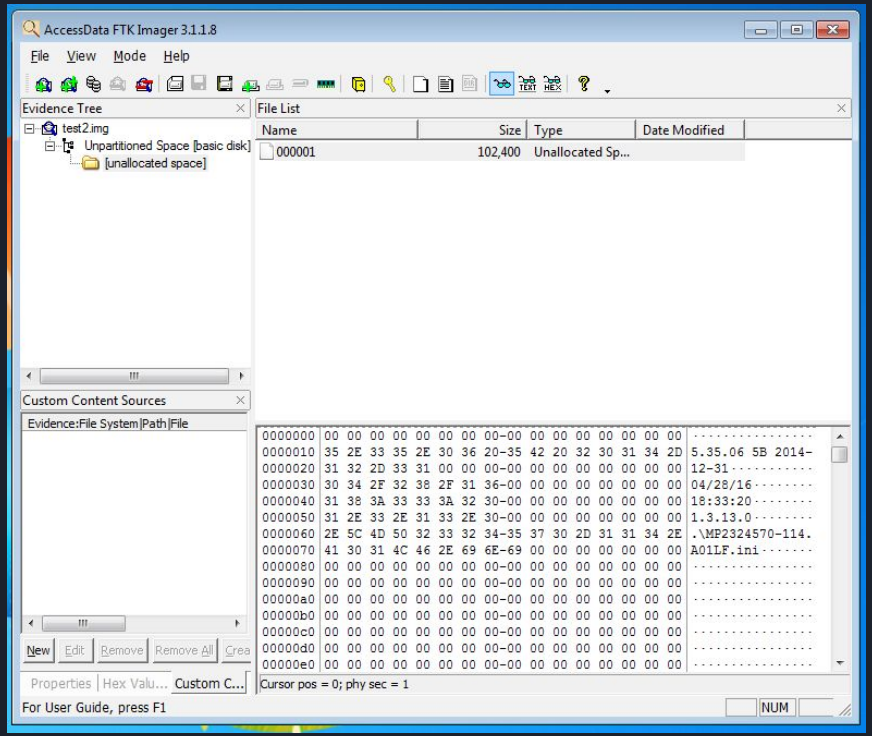
PhotoRec

- File carving tool specifically for images
- Carves segmented files (unlike Bulk Extractor)



Forensic Toolkit (FTK)

- Commercial forensic imaging software
- Can be used for manual file carving



Scalpel

- Automated command line file carving
- Native to Linux, but can be ported to Windows

Terminal

```
sansforensics@siftworkstation -> ~
$ scalpel -h
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Carves files from a disk image based on file headers and footers.

Usage: scalpel [-b] [-c <config file>] [-d] [-h|V] [-i <file>]
               [-m blocksize] [-n] [-o <outputdir>] [-O num] [-q clustersize]
               [-r] [-s num] [-t <blockmap file>] [-u] [-v]
               <imgfile> [<imgfile>] ...
```

Exercise Time

Puzzle category:

- FileCarving

If you get bored:

- Capstone

Entry Point

Malware Analysis

Created by Aaron Pope | apope@lanl.gov

Malware Analysis

- Working with live malware is beyond the scope of this class
- However, when investigating an incident, you're likely to come across suspicious files and programs
- What can we do?

Malware Analysis

Plenty of commercial malware scanners available

- McAfee
- Norton
- Symantec

Your institution probably already deploys malware and other host-based detection systems

Malware Analysis

Signature-based detection looks for strings of binary data that has been found in malware

```
strings:
    $text_a = "wire transfer"
    $text_b = "CEO"
    $hex = { E2 34 A1 C8 23 FB }
```

Malware Analysis

Behavior-based detection looks for malicious activities in running processes

- Deleting or encrypting files
- Opening network connections
- Downloading more programs

Can detect malware that has been slightly altered, but still behaves maliciously

Malware Analysis

What if the malware is brand new?

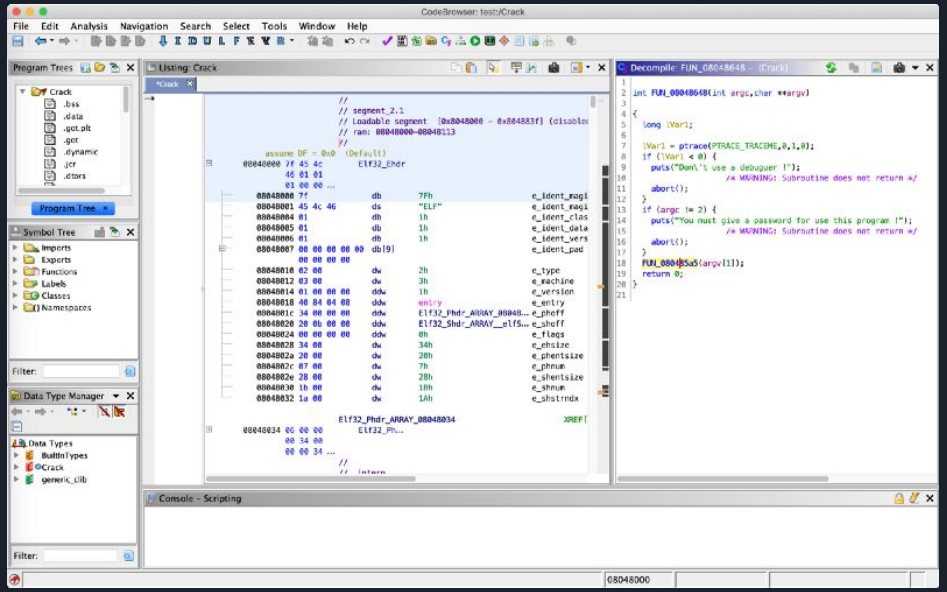
- Zero-day
- Not found in signature databases
- Behavior might be targeted at an organization
- Hand-crafted to elude detection

Bring in the malware analysis experts!

Malware Analysis

Static Malware Analysis:

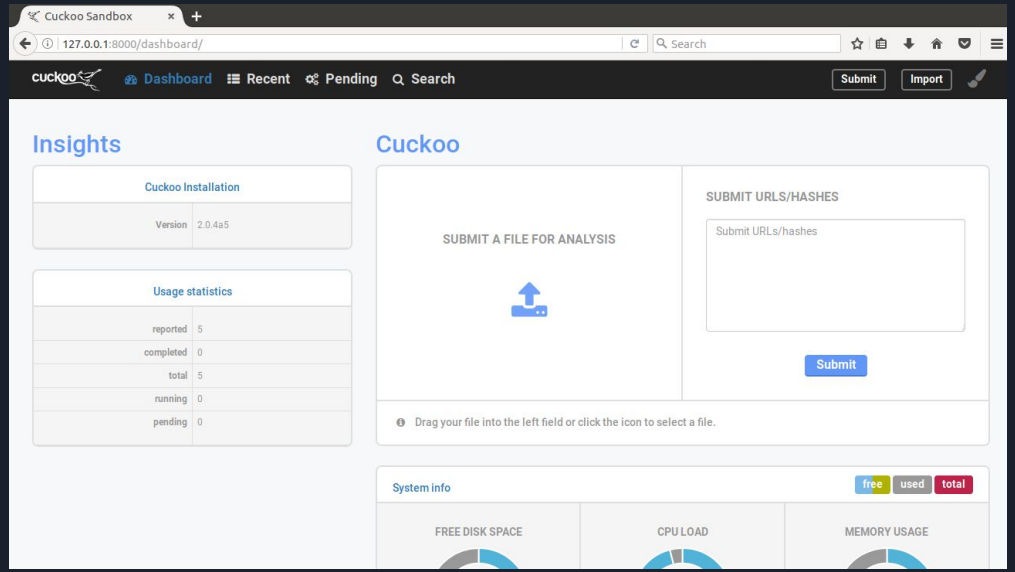
Reverse engineer the executable to get source code that is easier to understand than machine language



Malware Analysis

Dynamic Malware Analysis:

Put the suspicious program in a contained environment and run it, watching what it does

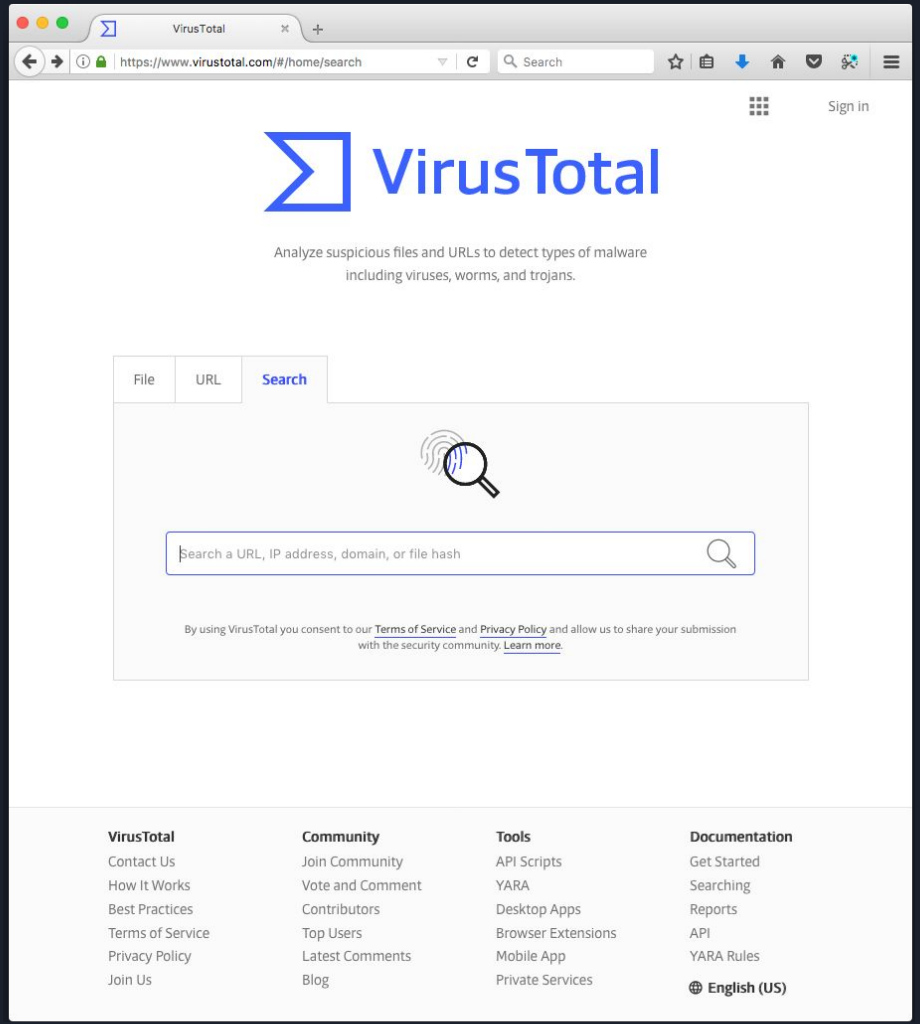


VirusTotal

https://www.virustotal.com/

VirusTotal, a subsidiary within the Google companies (Chronicle LLC, and Alphabet), is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners.

It's a place you can search for, submit, and have your files analyzed *for free.*



VirusTotal and Operational Security

VirusTotal and confidentiality from https://www.virustotal.com/en/about/

...Additionally, **all files and URLs enter a private store that may be accessed by premium (mainly security/antimalware companies/organizations) VirusTotal users so as to improve their security products and services.**

New language: YOU FURTHER AGREE THAT YOU WILL ONLY UPLOAD SAMPLES THAT YOU WISH TO PUBLICLY SHARE

How is this a problem for operational security (Ops Sec)?

VirusTotal and Operational Security

How is this a problem for operational security (Ops Sec)?

- Accidental upload of PII
- Unwanted disclosures of sensitive or proprietary data
- Malware targeting specific sites
    - Announcing to the threat actor you think there is a problem

Can VirusTotal still be helpful?

- Probably, through the use of file hashes
- You'll learn more in the exercise

Exercise Time

Puzzle category:

- MalwareAnalysis

If you get bored:

- Capstone

Entry Point

Incident Reporting

Created by
Shannon Beck | shannon@lanl.gov
Pablo A. Arias | arias13@llnl.gov

Who do you report to?

- Different names and different functionality
- Common names
  - SOC: Security Operations Center
  - NOC: Network Operations Center
  - CIRT: Computer Incident Response Team
  - CSIRT: Computer Security Incident Response Team
  - ?? What are your network security folks called?

What to submit?

Depends on who you are submitting to and what you are submitting.

- Suspicious email
- Questionable document
- System memory image

Once you *suspect* something is wrong…

Report it according to your local policy!

Ask the right questions

Who, what, why, when, where and how around an event or incident should include but is not exclusive to the following questions:

- **Where** did the analyst look for the data?
- Were there any suspicious file executions?
- **How** did the analyst identify hosts involved in the incident?
- Is there any traffic to the IP or domain?
- Where was the origination of the alerts? Should that be of more concern?
- **What** is causing the alert? Is it normal or suspicious?
- What actors are involved in the activity? Who are the users involved?
- **Who** received the suspicious emails?
- The questions need to be communicated clearly in the documentation as well

Data – Where Did it Come From?

- Document where the data came from!
- Follow local procedures
  - Memory image? From what system?
  - Disk image?
  - What process / tools did you use?

Notified that 192.168.0.2 (hostname: magicDog.cyberfire-training.org) was sending what looked like Command and Control (C2) traffic. Remotely logged on to the host via [Encase / Remote Desktop / another tool]. Used [FTK Imager Lite / RedLine / Encase] to take a memory image.

The “How”

- How did the analyst identify hosts involved in the incident?
  - Is there any traffic to the IP or domain?
- The “how” can be just as important as the “what”
  - Searched the network logs and found traffic to suspected bad IP address [list IP / domain name here; IP addresses can map to many domain names]. The hosts communicating with that address are 192.168.0.2, 192.168.0.24, and 192.168.0.56.
- What process / tools did you use? Document!

The “When”

- When was the incident response team alerted?
- When were the files you are investigated created, modified, deleted?

Need to account for system time!

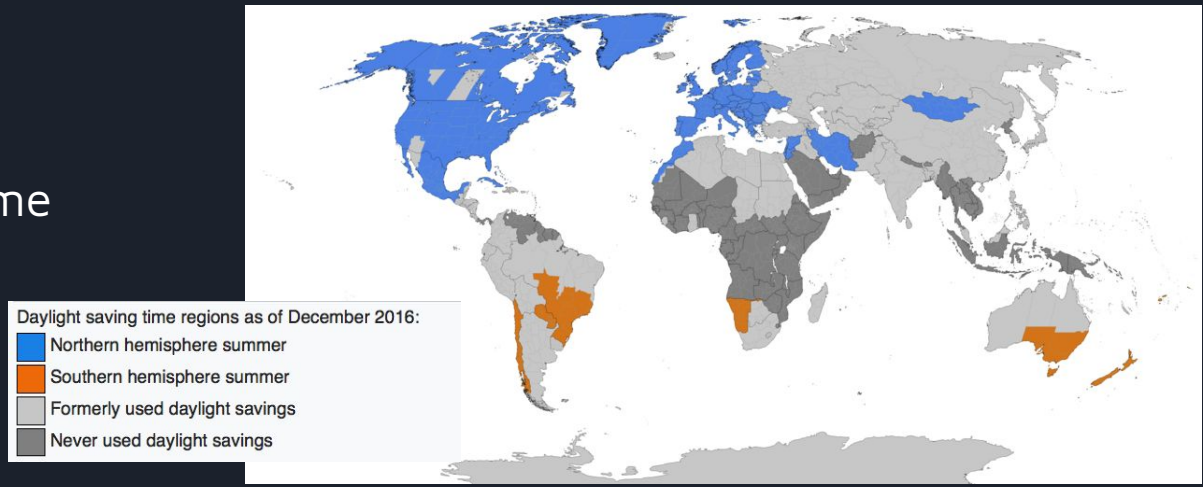
- Will impact things such as timekeeping, travel, billing, record keeping, forensic file information, anything with a timestamp.
- Not only do you need to be aware of your own time, but alternate time zones that will impact time correlation

Time Zones

When collecting evidence from a computer – know what time zone it is in

Daylight savings

vs. Standard time



Time – GMT, UTC, and Zulu

- UTC: Coordinated Universal Time (time standard)
- GMT: Greenwich Mean Time (time zone)
- "Z" (phonetically "Zulu") to refer to the time at the prime meridian (military/aviation)
- 2002-10-27 06:00:00Z

Time Drift

- Need to be wary about time drift
- Systems will not always keep the correct “true” time
  - NTP - Network Time Protocol
- When an alert fires on a host is not always when another system may receive the alert
  - Sending and receiving alerts takes TIME
- Consider any issues that could impact recorded time:
  - Log backfill
  - Network range
  - etc

Common Sensors and Alert Sources

IDS/IPS device and signature type (Snort, BRO, etc.)

Host-based detection (Windows logging via WLS or Sysmon; host-based tools such as MIR, Carbon Black, Encase, etc.)

Network traffic visibility (proxies and types, SSL /TLS visibility, IP and domain monitoring and block options)

Alert Origins

Where is an alert coming from?

- External source
- Internal source
- Security appliances (F5, Palo Alto, FireEye, ...)

What process / tools did you use? Document!

Users or Threat Actors Involved

- What users or threat actors are involved in the activity?
- Lateral movement in the network?
  - Does one user suddenly login to 100 hosts in under 1 hour?
- External users logging in from unusual geo locations?
- Attacker attribution
- “Bad” users shows history of:
  - Downloading malware / adware / spyware
  - Phishing attack
  - Gave login credentials at spoofed login page for a legitimate account
- Protect user and host information
- ***Caution:*** Attacker attribution can change classification levels

Phishing


Phind the phish
"Phishing" is when email purporting to be from a legitimate source attempts to trick you into volunteering your personal or credential-related information.
These messages vary in content, but all claim to be from legitimate sources such as E-Bay, your bank, PayPal, or a university group.
If you receive such a message, you should forward it as an attachment to phish@unc.edu.
ITS
INFORMATION TECHNOLOGY SERVICES

Phishing

Emails crafted to appear from legitimate sources

Major vector of infection

- In one study, 45% of the members clicked on unknown links in emails
- *https://blog.barkly.com/cyber-security-statistics-2017*

Document?

Document!

Then inform the right parties and share what you know and have documented.

Exercise Time

Puzzle category:

- IncidentResponse

If you get bored:

- Capstone

Entry Point

Wrap Up

Created by Aaron Pope | apope@lanl.gov

The Capstone Module

- Investigate a mock mini-incident
- Use your new skills
- A couple additional tools introduced

What Now?

- Cyber Fire Foundry is held multiple times a year
- Host Forensics
  - Memory and disk imaging an analysis
  - Digging into process, services, and registry
- Network Archeology
  - Finding adversary activity on a network
  - Unwrapping custom obfuscation protocols
- Malware Analysis
  - Reverse engineering malicious software
  - Analyzing executables' dynamic behavior
- Others:
  - Incident Coordination
  - Operational Technology

Contact Us!

- Don’t hesitate to reach out to us!
- Aaron Pope (LANL) apope@lanl.gov
- James Wernicke (LANL) wernicke@lanl.gov
- Pablo Arias (LLNL) arias13@llnl.gov
- Heather Keaty (LANL) hkeaty@lanl.gov

Surveys, Please!

Thanks for coming!